Office of the
Privacy Commissioner
of Canada

REPORT ON THE 2010 OFFICE OF THE PRIVACY COMMISSIONER OF CANADA'S

CONSULTATIONS ON ONLINE TRACKING, PROFILING AND TARGETING, AND CLOUD COMPUTING

TABLE OF CONTENTS

FOREWORD

In early 2010, the Office of the Privacy Commissioner launched a consultation process on online tracking, profiling and targeting, and cloud computing. Our goal was to shine a spotlight on evolving technological trends and to engage the public and stakeholders on the privacy implications of the online world. I think the consultations were a positive first step in this direction.

On behalf of the OPC, I would like to express our gratitude to the associations, organizations, advocates, academics and individuals who took the time to provide us with submissions, participate in the public events, or respond to our draft report. We appreciate their interest in these important public policy issues and were pleased to have the benefit of their views.

I would also like to thank the OPC staff for their hard work and commitment to this undertaking. In particular, I would single out the former Assistant Privacy Commissioner – PIPEDA, Elizabeth Denham; the former Director of Research, Education and Outreach, Colin McKay; Director of Policy and Parliamentary Affairs, Ann Goldsmith; Manager, Strategic Research, Melanie Millar-Chapman, for their leadership throughout this process. I would also like to thank Strategic Policy Analyst, Barbara Bucknell, for drafting this paper.

The following report on the consultations summarizes what we heard both during the consultations and in the responses to our published draft report, what we think, and where we would like to focus our future work. We look forward to continuing the work we started in 2010 and to advancing the discussion about privacy online.

JENNIFER STODDART
Privacy Commissioner of Canada

May 2011

EXECUTIVE SUMMARY

In the spring of 2010, the Office of the Privacy Commissioner of Canada (OPC) held consultations on online tracking, profiling and targeting, and cloud computing. The OPC received in total 32 written submissions and held public events in Toronto, Montreal and Calgary, attended by representatives of other privacy commissioner offices and industry, as well as academics, advocates and members of the public. On October 25, 2010, the OPC released a draft report on the consultations, seeking further comments on a range of issues, from the public/private divide to cloud computing. Twelve responses were received, addressing some of these issues.

With respect to online tracking, profiling and targeting, we heard primarily about the privacy issues related to behavioural advertising: what it is, what the benefits are, what risks to privacy exist, and what self-regulatory measures are in place. In terms of general privacy concerns, the blurring of the public/private divide and its effects on reputation was seen as a significant issue that arises from online tracking, profiling and targeting. Children's activities online and the need to incorporate privacy into digital citizenship programs were also items that were raised.

The consultations were an opportunity to examine the practices of online tracking, profiling and targeting through the lens of the *Personal Information Protection and Electronic Documents Act* (PIPEDA). While most industry participants were of the view that PIPEDA can handle the evolving technological environment, certain challenges with respect to applying the law were raised by many respondents and participants. Defining what is (or is not) personal information; determining the appropriate form of consent; limiting the use of personal information; implementing reasonable safeguards; providing access and correction to online information; and ensuring accountability were cited as PIPEDA-related issues that need careful attention. Online tracking, profiling and targeting are still largely invisible to most individuals, and most respondents and participants agreed that greater transparency is needed for the benefit of individuals and to ensure innovation.

With respect to cloud computing, the OPC learned about the different characteristics and models of cloud computing. We heard about its benefits and risks to enterprises and consumers. Again, most respondents and participants were of the view that PIPEDA can address issues that arise from cloud computing while others suggested that more should be done. Most of the PIPEDA-related issues concerned jurisdiction and availability of personal information to third parties; safeguards; new uses for the personal information and retention; and access.

The OPC is proposing to undertake specific activities in relation to online tracking, profiling and targeting, specifically in terms of research and outreach activities, as well as policy development. The OPC also intends to reach out to individuals and small and medium-sized enterprises with respect to privacy issues related to cloud computing. The comments related to PIPEDA compliance will also be considered in any review of the legislation.

PREAMBLE

To set the stage for the discussions during the Office of the Privacy Commissioner of Canada's 2010 Consumer Privacy Consultations, we constructed scenarios about real-life activities that Canadians perform daily. Our purpose was to make the frequently technical and abstract concepts of online tracking, profiling and targeting, and cloud computing more tangible for Canadians. This was intended to engage individuals, industry and privacy advocates in a dialogue about how everyday actions online implicate Canadians' privacy, and what is being or should be done to protect it. These scenarios are used throughout the report.

Please note: Brand names of popular sites are used in this report for simplicity's sake. There is no intent to comment on or make suggestions about the privacy practices of the named sites.

"LOUISE AND DAVID'S WORLD"

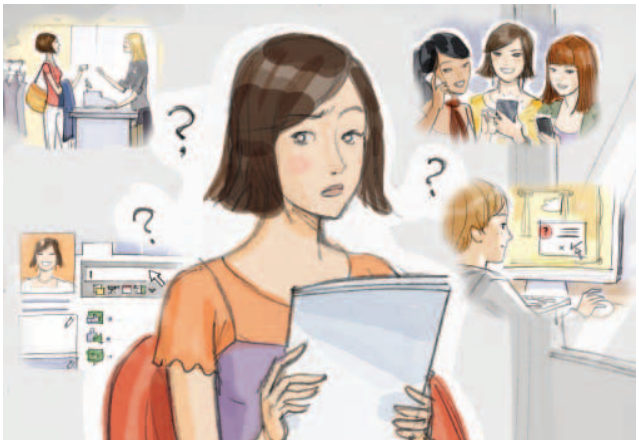
Louise is a 21-year-old college student who likes to meet people and try new things. She is active online, using the Web for everything from buying trendy clothing and concert tickets to keeping in touch with friends by posting updates and photos to her Facebook page. Now in her final year of college, Louise is starting to look for a job. She is putting herself through school by making jewellery and selling it online. She also collects specialty comic books and belongs to an international network of comic book enthusiasts. Louise has a younger brother, David, who is nine years old. David loves online games and signs up for them on his own, but uses his sister's credit card for any purchases.

Now and then, Louise wonders what these online companies do with the information she gives them. She has heard some people talk about "privacy online" but she isn't sure what that means. One time, she noticed a link to a privacy policy on a website. She clicked on it, tried to read it, but became bored with it. It seemed like a bunch of legal talk. She gave up and continued with her activities.

I.I Introduction

Louise and David are typical Canadians. They are among the millions who connect to the Internet every day to shop, talk to others, play games, or, like Louise, conduct business. They see the advantages of life online, and as younger Canadians, Louise and David have integrated the virtual world into their real-world experiences. They do not remember a time of paper files, typewriters, fold-up maps or lining up to buy movie tickets. They live an on-demand life, with instant access to all sorts of information—what their friends are up to, where they can find the best deals, and whom their favourite rock star is dating. They run their social lives online; they upload their photographs, videos and opinions; and they feel part of a community that spans the globe. If they are old enough, they pay bills, apply for credit, or run businesses. Music, videos, films, books, clothes, newspapers, games are a click away. And access to much of this is free, at least in the monetary sense.

Canadians of all ages see the value that technology brings to their lives—convenience, connection, creativity—and are embracing it. That does not mean, though, that Canadians like Louise never consider what goes on in



the background of their web activities. Where does the information go? Who looks at it? Louise seeks answers but finds information hard to find or confusing and more complex than she thought. Perhaps Louise senses that she is missing the bigger picture. But where can she go to find the "big picture"? The technology is so easy to use, she thinks, so why is it so hard to understand how her personal information fits in?

I.II Privacy protection in Canada

Fortunately for Louise, there are laws in Canada about how her information is treated, and there is an office that helps oversee compliance with those rules. The mandate of the Office of the Privacy Commissioner of Canada (OPC) is to oversee compliance with the *Privacy Act*, which applies to the personal information handling practices of federal government departments and agencies, and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), Canada's private sector privacy law. PIPEDA applies to organizations that collect, use and disclose personal information in the course of a commercial activity (unless substantially similar provincial legislation is in place).[1] PIPEDA also covers the personal information of customers and employees of federal works, undertakings and businesses. Generally speaking, PIPEDA would apply to the personal information handling practices of private-sector organizations engaged in online tracking, profiling and targeting, and cloud computing.

The mission of the OPC is to protect and promote the privacy rights of individuals. To that end, the Office seeks opportunities to promote public awareness and education of privacy rights and obligations through engagement with federal institutions and bodies, the private sector, a wide range of other interested stakeholders, and the public at large. If Louise wanted to, she could visit our website, call us with her questions, or file a complaint if she was concerned about something one of the companies she dealt with was doing. Among its many functions, the OPC investigates complaints; responds to inquiries from individuals, Parliamentarians and organizations seeking information and guidance; proactively engages with stakeholders; provides public education materials and guidance documents; monitors trends; and works with privacy stakeholders from other jurisdictions in Canada and internationally to address global privacy issues that result from ever-increasing transborder data flows.

I.III New technologies, old questions

Changes in technology in the second half of the 20th century drove many countries to develop privacy legislation. Concerns were being raised about the potential effects of rapidly evolving technologies on privacy. As computers and databases grew more powerful, academics, policy makers, governments and international organizations began to consider how best to protect the privacy of individuals. In Canada's private sector, a self-regulatory code was developed in the 1990s that was largely based on the fair information practices outlined in the 1980 OECD *Guidelines for Governing the Protection of Privacy and Transborder Flows of Personal Data*. In 2000, PIPEDA was passed, incorporating the self-regulatory code into the legislation. The fair information practices, found in Schedule 1 of PIPEDA, are: accountability, identifying purposes, consent, limiting collection, limiting use, disclosure and retention, accuracy, safeguards, openness and individual access.

The majority of issues that the OPC focused on in the early years of PIPEDA concerned the personal information practices of bricks-and-mortar organizations such as financial institutions, telecommunications companies, credit bureaus or transportation companies,[2] and involved everyday business transactions. Such issues included, for example, what constitutes personal information and what is the appropriate type of consent, while others focused on the implications of technology in the handling of personal information matters, such as whether cookies were personal information.[3] The interpretation the OPC took in considering these issues has provided the framework through which we examine the privacy practices of today's evolving business models and the effects of new technology on certain practices. This has worked so far because the law is principle based and technology neutral.

Technology has changed, and so too have our interactions with it. When PIPEDA first came into force in January 2001, there were no social networking websites, no video sharing sites, no microblogging. The World Wide Web was growing and businesses were moving online; mobile phones were not in wide use but were becoming popular; surveillance cameras were becoming increasingly prevalent; and the specter of biometrics was starting to take shape. Some Internet forums, where people could communicate with each other, existed, but by and large, communication online was one-way—from website to individual.

Today, individuals play a different role in personal information sharing. In the early years of PIPEDA, an individual like Louise for the most part had to leave her home to participate in commercial activities. Now, she can conduct most of her commercial activities, even her work tasks, from home. The growth in opportunities to share personal information about ourselves and others online—to an often invisible audience—helps make it more challenging to maintain a divide between our public and private lives, and our work and personal lives. Sharing information about ourselves or others is nothing new, but doing it online means that there is a permanent record of it. And increasingly, industry is finding ways to capitalize on this record.

This evolution has implications for privacy protection. The OPC has a responsibility to Canadians and to Parliament to monitor emerging privacy issues and to take proactive steps to inform them of these changes. The pace at which technology is changing makes it even more critical that our Office have a strong understanding of emerging trends. We need to keep abreast of the potential privacy implications of technology, as well as the changing role of the individual in creating and disseminating personal information.

I.IV Will the tools we have now be enough to protect privacy in the future?

In terms of personal information protection, Canada has been a leader in providing a privacy framework that protects the privacy of individuals and supports organizations in doing so. As technology advances and the digital economy evolves, it is important to ensure that the balance between the needs of business and the privacy rights of individuals is maintained and reinforced where needed. So far, PIPEDA has been working well, and it has been able to adapt to technologies and business models that did not exist when it first came into force. PIPEDA has also been found to apply to foreign entities that have a real and substantial connection to Canada—an important fact considering that Internet activities are mostly borderless. It is important, however, to ensure that Canadians continue to enjoy privacy protection while also taking advantage of emerging trends and technologies. It is important, too, that innovation continues in order for industry to thrive.

2010 Consultations

For these reasons, the OPC decided to hold consultations with Canadians on issues that we feel may pose challenges to the privacy of consumers, now and in the near future.[4] As we noted in our submission to the Government of Canada's consultation on a digital strategy, we are on the cusp of a convergence of technologies that will provide comprehensive "dataveillance"[5] of individuals. The aim of this consumer consultation was to learn more about certain industry practices, explore their privacy implications, and find out what privacy protections Canadians expect with respect to these practices. The consultation was also intended to promote debate about the impact of technological developments on privacy, and to inform the next review process for PIPEDA.

We chose to focus on online tracking, profiling and targeting, and cloud computing because we see these trends as likely to have impacts on the privacy of Canadians. As people and businesses increasingly move online and enjoy the many benefits of the digital age, the practices that support the services people like need to be examined in full from a privacy perspective.

We also focused specifically on children online, such as David. The average age of children who use the Internet appears to be dropping,[6] and the implications on their privacy need careful attention from public policy makers. One of our goals is to draw attention to this issue. Traditionally, the focus has been on ensuring that children are safe from predators as they navigate the Web. Many experts have stated that ensuring children's personal information is protected is an area that needs more attention.

In recent years, the OPC has examined the privacy practices of social networking sites and dealt with issues arising from street-level imaging technology used to map Canada's cities. In 2008 and 2009, we examined the use of deep packet inspection through investigations into its use and submissions to the Canadian Radio-television and Telecommunications Commission, and by commissioning a series of essays on the technology. In December 2009, we participated in the Standing Senate Committee on Transport and Telecommunications hearings on the digital society, where we touched on privacy and security in the digital world. In reflecting on what we had learned from this work, we decided that we needed to engage the public, engage stakeholders and educate ourselves further on the privacy implications of living our lives online. In particular, the evolution of Web 2.0 has underscored the need to find innovative ways to reach the public in order to help them navigate the Web in full awareness.

We wanted to hear from Canadians. We wanted to speak to those in the industry about their practices and how they see privacy in relation to technology and innovation. We wanted to hear the views of academics, who are engaged in reflecting on privacy and technology and where we might be headed, and of advocates, who play an important role in providing a voice for Canadians on a subject that is becoming increasingly complex to navigate.

Given that technology has largely erased borders when it comes to data processing, the OPC recognizes that international co-operation and consensus on privacy issues

is vital to helping protect the personal information of Canadians. Many international organizations, policy makers and other data protection authorities are also taking a closer look at the personal information protection principles that have formed the basis of legislation or self-regulatory efforts, to see if they will serve citizens well in the future. Some are also examining many of the same issues discussed in this report. We are monitoring their efforts, and they ours. Indeed, we were honoured to have David Vladeck, Director, Bureau of Consumer Protection of the U.S. Federal Trade Commission (FTC), join our consultation event in Toronto on April 29, 2010. The FTC conducted roundtables on privacy in late 2009 and early 2010, and on December 1, 2010, released its proposed framework for businesses and policymakers.[7] We were also very pleased to welcome a number of U.S. and European industry leaders and academics to our events. Their perspectives on these issues are highly valuable as we strive to find common approaches to privacy protection.

We held the consultation events across the country to reach out to Canadians and to target those areas where many of the industry associations or businesses are located (or are relatively close to). We webcast the event and relied on social networking tools of our own to elicit interest in as large a number of Canadians as possible.[8] On October 25, 2010, we issued a draft version of this report for comment, asking for feedback on specific issues. Not all issues received comments. However, the issues remain highlighted within the report (and summarized in Appendix A) as we think that they merit continued consideration. We received 12 responses on the draft, the substance of which has been incorporated into the text of this report.

We intend the consultations and this report to be a springboard for new outreach activities for the OPC to pursue in fulfilling our mission to promote public education on privacy rights.[8] Outreach involves speaking to Canadians, and it also involves educating organizations on their privacy obligations. The consultations will contribute to the development of the materials that we use to conduct our outreach activities. They will also inform our research and policy work over the next few years. They will help shape the Office's input into the next parliamentary review of PIPEDA.

The consultations, at times, raised more questions than they answered, but they provoked some stimulating discussions about where we think privacy is being challenged. This report is not intended to be a "finding" into certain practices; rather, it attempts to place the practices into the PIPEDA framework to highlight where there may be concerns. It also notes areas that touch on more general privacy issues, not necessarily those that are covered by the legislation. There was often general agreement on privacy implications, though there were differences on how to address them. This report is also intended to summarize the various positions and suggestions that we received from stakeholders.

The report also signals the areas where we intend to take action or study further, and where we think industry and government need to focus their attention. The report is not our contribution to the PIPEDA review process and does not contain specific changes to the Act that we would like to see. We heard some suggestions on changing the Act, and we will take these into consideration when we embark on the next PIPEDA review process.

Individual Canadians, Commissioners' offices, business, government, academia and advocates all have a role to play in personal information protection. This report is the OPC's contribution to the study of the privacy implications of new technologies and the online world. We hope it will generate an important discussion about what privacy protection means in the 21st century.

ONLINE TRACKING, PROFILING AND TARGETING

Shopping at her local mall, Louise buys some designer jeans at a store[9] with her credit card. She also has the clerk swipe her loyalty card.

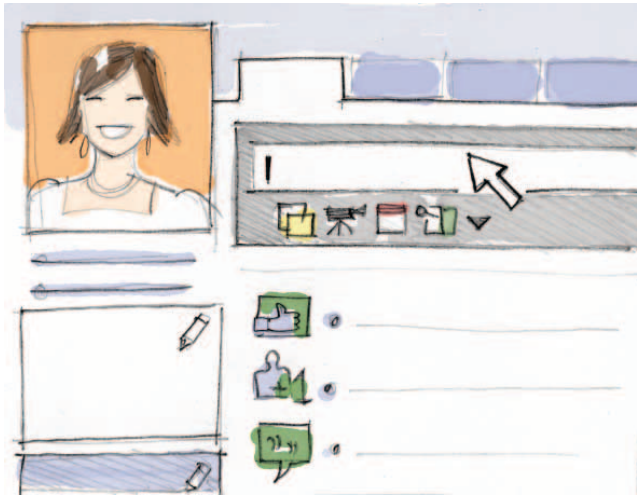
When Louise arrives home, she signs in to her new account at the store's website to learn more about the clothes she had tried on but not bought. In her excitement to see the store's merchandise, she clicks through the site's lengthy privacy policy without reading.

In searching the store's website for a blouse to go with her new jeans, Louise sees an advertisement for jewellery that really appeals to her, so she clicks on it. Louise feels comfortable at the small Canadian jewellery website because the design of the site makes her feel as though she is visiting a friend's page.

She also likes the styles of jewellery on the site, so she buys a necklace and clicks on the "Like" button to update her friends on her latest purchase. From there,

she leaves the site and searches for the listing of a concert, and buys two tickets. After that, she checks the status of the online auction she is participating in to get a new specialty comic book.

Louise then updates her Facebook page to let her friends know about her purchases and to see who else will be attending the concert. From Facebook, she checks out her favourite online bookstore, where she purchases a book that was recommended to her by another comic book expert.



When Louise bought the jeans, the store offered her a widget application for her iPhone for the duration of her shopping trip in the store to show her the location of clothing she might like based on her gender and her age (21 years). Louise opted for a more personal experience by adding her e-mail address, phone number and the clothing styles and sizes she prefers.[10]

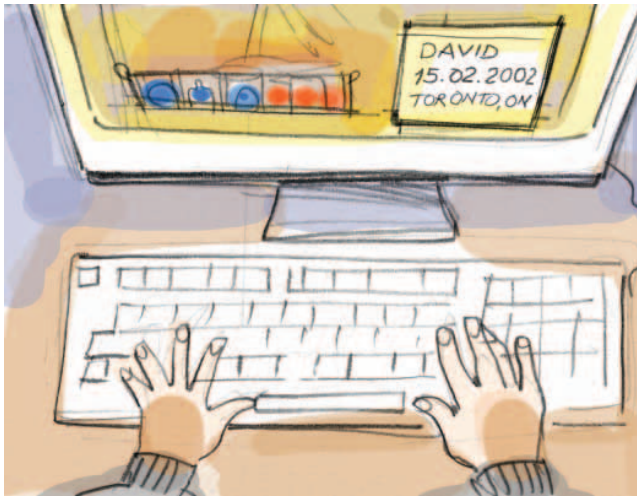
While she was in the store, Louise also checked in through a popular location-based service and then got a message on her iPhone that the coffee shop beside the store was offering a special lunch deal with some of her favourite foods—a Chai green tea and a sprout sandwich with Gruyère cheese.

Later that evening, Louise goes out with friends and wears her new outfit. She and her friends check in through the location-based service and then receive offers for discounts at local restaurants and nightclubs. They pick an offer and alert other friends to the deal. They are eager to get on with their night.

Louise's younger brother, David, is 9 years old. He loves online gaming and has signed up for several on his own. He gets annoyed with any notices and clicks through them as fast as possible. He sometimes asks Louise for her e-mail address and credit card number so he does not have to involve his parents in the consent process. She is fine with this arrangement, other than the e-mails she now gets for special offers related to the games.

When David signs up for games, he tends to fill in all the fields, because he's not sure if he can leave them blank, though sometimes he makes up information. He likes to chat with other players, and if he trusts them, he reveals information about himself, like where he lives and what he likes to do.

One of the games David likes to play has posted a notice that "non-personal" information would be collected at log-in, and that consent for this had already been received in the Terms of Service. This satisfies David and he does not inquire further, as he is not concerned anyway. However, the definition of "non-personal information" in the Terms of Service refers to the collection of David's computer's IP address, which some people consider to be personal information.



II.I What is online tracking, profiling and targeting?

What happens when Louise travels across the web, when she's clicking on advertisements, making purchases and letting her friends know about them? How does the advertiser or data broker know that Louise likes jewellery, for example? Does the loyalty card information ever get married up to her online activities? What about the information she provides through the widget or on her Facebook page?

Everything you do online is recorded in some way. And some of this information is increasingly being gathered and used for commercial purposes (and for government programs as well). Data is big business, with money to be made from the personal data emissions scattered around the Internet by people like Louise and David.

How does tracking and profiling work?

When organizations track Louise online, data about her browsing habits are collected through digital markers. HTTP cookies, Flash cookies and web beacons are currently the most common ways user information is gathered. Cookies are small text files that are placed on Louise's computer's hard drive when she visits websites. They collect and store information about her based on her browsing patterns and any information she provides. Flash cookies can be used to save state information between sessions, but they are also used to track the websites that Louise visits. Flash cookies are popular with websites, are often used along with more traditional web cookies, and can be used to recreate web cookies if the latter are deleted. Web beacons "are small strings of code that provide a method for delivering a graphic image on a web page or in an e-mail message for the purpose of transferring data....Frequently, the web beacon is designed to blend into the background of the page being visited."[11] Beacons can be used to understand certain patterns of use by a site visitor; they can also be used to deliver cookies or downloadable applications.[12] While Louise can turn her cookies off or periodically clear them, it is hard to opt-out of or refuse web beacons. Super cookies are another type of cookie that is emerging. These use new storage locations built into browsers to save information about a user.

The types of information collected in log files about Internet users can include: Internet Protocol (IP) address; pages visited (on a single site or across sites); length of time spent on pages; advertisements viewed; articles read; purchases made; search terms or other information entered on a site; user preferences such as language and web browser type; operating system; and geographical location information, through IP addresses (on the web) or the Global Positioning Systems (GPS) common in many mobile communications devices.

Additional data may be gathered using other technologies, such as deep packet inspection. Individuals like Louise also volunteer significant amounts of personal information, especially through their participation in social networking sites such as Facebook, MySpace and LinkedIn, and other popular web-based services such as Foursquare. Data mining techniques are then used to uncover patterns from the data, which can then be used for various purposes.

II.II What we learned

We received 21 written submissions on online tracking, profiling and targeting. The primary focus in the written submissions was on behavioural advertising. Other possible uses of the information were discussed during the panels. Of the 12 responses to the draft report, nine referenced online tracking, profiling and targeting.

What is behavioural advertising?

Several terms are used when talking about online advertising: demographically targeted, location, behavioural/interspace, interest-based advertising. These are all variations on behavioural advertising.

Behavioural advertising consists of tracking consumers' online activities over time in order to deliver advertisements that are targeted to their inferred interests. Behavioural advertisers use this data to build user profiles, determine user interest categories and show ads based on demographics and assumptions about user interests. Depending on the advertiser, these interest categories can be broad (e.g., car enthusiast) or very specific (e.g., young female Honda owners with small children living in Alberta). Interest categories are used to select and serve advertisements that the advertiser has defined as relevant to those categories.

Information about the online behavior of Louise can be used to maximize her engagement with products and services. With the rise in popularity of mobile devices, advertisers are increasingly focusing on location as a way of creating potential new customers. Location can be derived from cellular networks, WiFi access points, satellite links and Global Positioning Systems to deliver services to mobile devices. Louise also volunteers her location when she uses location-based services, such as applications that recommend nearby restaurants or keep tabs on the whereabouts of friends.

One important term that is distinct from behavioural advertising is "contextual advertising." The FTC, which has been studying the practices around online advertising for some time, defines contextual advertising as "advertising based on a consumer's current visit to a single web page or a single search query that involves no retention of data about the consumer's online activities beyond that necessary for the immediate delivery of an ad or search result."[13] It is not considered as privacy invasive as behavioural advertising because it does not involve the collection or retention of an individual's online behaviour—browsing, location information or social networking site activities—over time. However, once an individual clicks on a contextual advertisement, this action is tracked and may be used later to serve a targeted advertisement.

Who are the key players in delivering online behaviourally targeted advertisements?

There are typically three main players in the behavioural advertising model: websites, advertisers and ad networks. Simply put, websites need money to operate, advertisers want to sell products, and ad networks help deliver

advertisements to a target audience. The submissions and panel discussions did not detail the variety of players that can be part of the online tracking, profiling and targeting environment.

In reference to the current "online advertising ecosystem," one of the submissions we received noted that in recent years the number of advertising networks has decreased. This is making it possible for a small number of very large advertising companies to broadly track user behavior across the Internet. Many of these advertising networks are owned by the same entities that provide a number of web-based services and have a direct relationship with users.

Benefits and risks

The industry associations we heard from cited the many benefits of behavioural advertising. They argued that while individuals do not have to pay (at least in the monetary sense) for some information and services on the Internet, revenues nevertheless have to be generated. Advertising is the key source of revenue for web-based companies. Advertisers are looking for the best way to market products and services, and those paying for advertising want their products and services to reach the greatest number of interested parties. Citing some studies that indicate people prefer to receive information that is of interest to them, the associations noted that behavioural advertising provides users like Louise with marketing information that is personally relevant. Other benefits cited include support for cultural, sporting or other events; generating sales of goods and services; and supporting the economy and jobs in the marketing and related industries.

In some of the responses to the draft report, we heard further about the benefits of tracking, profiling and targeting. Advertising revenues have enhanced individuals' online experiences by financing a diversity of voices on the Internet. Other benefits for users include recommendations for products and services and website customization. In terms of benefits for small businesses, they can generate revenue in part because of new ways of carrying advertising on their sites. One company noted that with targeted advertising, advertisers can reach the same audience on niche (smaller) websites as on larger portal sites but at a lower cost. Without this, it stated, ad dollars would be diverted to larger and better known "publishers" that can deliver a larger audience. Small and medium-sized websites would have to switch to subscription models as opposed to free access models. This company contended that most publishing companies and ad networks would be forced out of business. One association noted that any undue restrictions on targeting will ultimately reduce the ability of online companies in Canada to provide valuable services to consumers both in Canada and around the world.

Many industry associations as well as advocacy groups and academics nevertheless noted that there are risks with respect to online tracking, profiling and targeting. Key industry associations acknowledged that about half of Canadians they surveyed express some discomfort with respect to being tracked online. Those industry associations that commented on the issue acknowledged that such practices risk losing customer trust, typically because the practice of tracking individuals is invisible to users. They referred to industry efforts at self-regulation and education of consumers as ways to increase visibility of the practice and to ensure that users' privacy is respected. These self-regulatory measures are discussed in more detail below.

Privacy or consumer advocates who provided written submissions and/or participated in the consultation events also noted many risks related to the practice. In the response to the draft report, an advocacy organization expressed the view that the business models built around online tracking greatly challenge the balance between e-commerce and privacy that underpins PIPEDA. Noting that in such models the user is not so much the customer as the product, the organization argued that revenues are dependent on obtaining more personal information and that the true customers are advertisers. As a result, the concept of legitimacy in terms of the purposes for collecting, using or disclosing personal information in PIPEDA is challenged.

Lack of awareness and understanding of the role and extent that "data collection plays in providing behavioural targeted advertisements and consumer tracking"[14] was a key concern expressed during the consultations. Another risk or concern raised was that such practices threaten the individual's ability to control the flow of their personal information. In one of the responses to the draft of this

report, an advocacy organization challenged industry assertions that individuals view advertising as a benefit; rather, it believes that users tolerate advertising.

Other risks raised include the use of potentially inaccurate data affecting users' online experiences, as well as decisions made about them—often without them being aware and, consequently, having no ability to challenge the accuracy of the information. Another significant risk is that profiling can be used to discriminate against individuals, for example through pricing schemes. In sum, these practices threaten consumer autonomy. These concerns are discussed further in the sections on general privacy issues and PIPEDA principles below.

Scope of behavioural advertising and the international context

One submission noted that behavioural advertising currently accounts for only 10% of online advertising revenues in Canada. Although the discussion about behavioural advertising focused on the Canadian context, the fact that online practices generally do not recognize borders was stressed. For this reason, many industry respondents noted that any discussion around what some of the best privacy practices should be needs to take into consideration various international requirements.

Self-regulation

We learned about the self-regulatory efforts of a number of organizations, many of whom operate in more jurisdictions than Canada. Generally speaking, these efforts are intended to provide information to consumers about online behavioural advertising activities and provide information to them with respect to their opt-out options. They centre on certain guidelines developed by industry associations in the United States and include the following principles: notice and choice, education, transparency, control, data security, material changes, sensitive data and accountability. Several submissions cited at least some, if not all, of these principles as guiding their online tracking, profiling and targeting activities.

II.III Canadians' views

The following is a brief overview of some relevant surveys related to views about privacy, including one commissioned by the OPC (we conduct a survey of individuals every two years), as well as a survey conducted by Natural Resources Canada on geospatial information. Some of the written submissions referenced specific studies on Canadians' attitudes to tracking and/or behavioural advertising. Two of these submissions were made public, and the studies referenced in the submissions are included below.

General attitudes toward privacy

A 2009 EKOS survey commissioned by our Office found that 90% of Canadians are concerned about the impacts of new technology. While individuals may not be aware of certain privacy risks or consciously accept a trade-off to their privacy, Canadians still have high expectations for privacy, including online, and worry about how their personal information is being used, especially if it involves transborder data flows.

People between the ages of 45 and 65 are particularly likely to be concerned about the privacy impact of new technologies, while those under 25 are less likely to express high levels of concern about the issue. Canadians under 25 are also less likely to be concerned about off-shore processing and storage of their personal information.

Overall, 98% of all Canadians believe that it is important to have strong privacy laws.[15]

Attitudes toward online tracking and targeting

According to a 2009 survey conducted by the Public Interest Advocacy Centre (PIAC) on online behavioural tracking, nearly 75% of respondents were either not very comfortable or not comfortable at all with tracking-based advertising. Awareness of tracking devices and techniques was split 50-50 between individuals who were aware and those who were not aware of such techniques. The study

found that individuals tended to be more comfortable with online tracking for customer service or advertising purposes if done by companies with which they have had prior dealings.[16] In a study conducted on behalf of the Canadian Marketing Association (CMA) in 2009 on behavioural advertising, it was noted that 50% of Canadians were "somewhat uncomfortable" with marketers using browsing information to serve more relevant ads.[17] In one study discussed during a panel discussion in Montreal, it was noted that individuals tend to become more comfortable with behavioural advertising once it is explained to them.

Attitudes toward geolocational privacy

In terms of location data, Natural Resources Canada conducted a survey concerning Canadians' views on privacy and the use of geospatial information. Some of the key conclusions in the study were that Canadians are fairly careful about sharing their location-based information and that control over the information being shared and the context are key drivers of individuals' comfort when faced with sharing location-linked personal information. Leading to higher levels of discomfort are "situations where information is being linked to one's real time location, being used for targeted marketing, where there is little or no control, being shared with the private sector or general public and for reasons related to economic activity…" Approximately half of the respondents did not perceive any benefits to location-tracking technology or were unsure what benefits it may provide.[18]

II.IV General privacy-related issues

"We are living our private lives online."
Jennifer Stoddart, Privacy Commissioner of Canada[19]

From writing about ourselves and others on social networking sites, to mapping capabilities that show us and others where and how we live, to connecting us to our friends, from the merging of what we like to where we are, to monitoring our use of the things we own—a comprehensive portrait can be drawn of an individual, thanks to increasingly powerful data mining tools. Moreover, advances in technology enable a convergence of capabilities on a single device, or the convergence of capabilities or services on a single platform. The latter scenario represents an amassing of information and power in increasingly small numbers of organizations and poses a significant challenge to protecting the online marketplace.

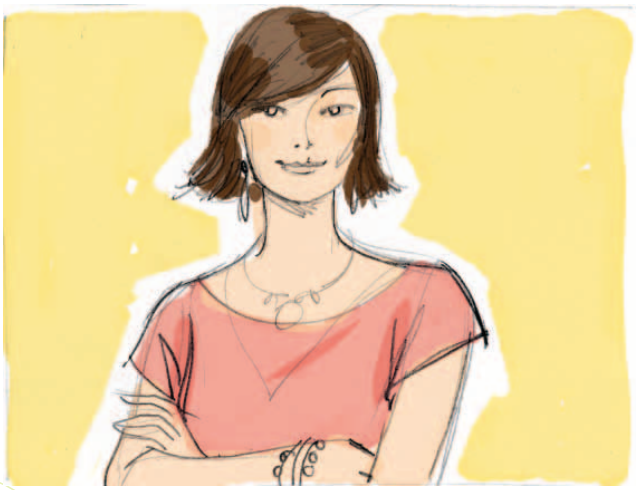
Individuals are enthusiastic consumers of technology and participants in the social web. They take advantage of the tools offered, but there are consequences—some social, some economic, some hurtful and some beneficial. Nevertheless, they are embracing these tools and sharing or creating increasing amounts of personal information. At the same time, they still say that they value privacy. This appears contradictory, but is it?

Many of the submissions and consultation panels raised "general" privacy issues, as well as issues related specifically to the scope and principles of PIPEDA. This section will cover some of the general privacy issues related to online tracking, profiling and targeting. Part of the comments in this section touch on matters related more generally to the phenomenon of individuals spending increasing amounts of time online and sharing greater amounts of personal information—both their own and that of others—with the online community. Issues raised in this section concern whether technology influences our behaviour, and if so to what extent. We also consider the observers—other people, advertisers, researchers, marketers, government—who use this information for a variety of purposes, with implications for our privacy, some of which do not fall neatly within the scope of PIPEDA.

WHAT WE HEARD

The blurring of the public/private divide and the effects on our reputations

Who is Louise?



There was much discussion on the panels in Toronto and Montreal about how the social nature of the current online experience is having profound effects on privacy. Some of the submissions we received and some of the comments we heard noted that, with the prevalence of mobile technology and increasing popularity of social networking, the traditional notion of public and private spaces is changing. Social networking provides individuals with the mechanisms to make their private lives more public, and this is contributing to shifting expectations of privacy. In turn, some social networking operators point to this shift to justify further openness and sharing. The use of mobile phones and the increasing availability of location-based applications further bring the public eye into the private realm.

There was some discussion about the "invisible audience," in other words, whom Louise believes she is addressing. This has a great effect on the type and amount of information that is disclosed. The differences in perception of just what audience the individual is addressing are most keenly seen in the case of children and young adults. When younger children, such as David, are online, they expect "the public" to be composed of other kids. They do not expect adults to be part of that public, even though they know that adults can see the information. Young adults are likely to post information that promotes the identity they want to project to the audience. This explains some of the social information uploaded by certain kids who feel a need to be popular.

It was noted that people have difficulty visualizing their audience when uploading information about themselves (or others). They are alone, facing a screen, and because of the solitude of the activity, it is easy to misjudge their audience. Interacting online makes people behave differently too, and social norms are being challenged. For instance, when considering the issue of tracking and geolocational technology, not only can businesses (and, by extension, government agencies) track individuals, individuals can track each other. And because individuals have the capability to do so, "tracking (of others) not only becomes socially acceptable, it becomes social."[20]

There was discussion too about the effect that peer pressure and power relationships have on individuals like Louise and David, and how it undermines standard privacy protections, such as consent. People feel compelled to join many of these services, fearing that if they do not, they will be "left behind." Some panelists commented on how much our social lives rely on the use of information technology; in turn, through technology, our connections to others can be mapped. One consequence of this is that individuals are being typecast based on whom their friends are. We will return to the use of social media marketing later in this paper.

When barriers drop but perceptions do not, and people post online as though they are writing in their diaries, there are very real risks to their reputations. In addition to the personal risks, it was noted on one of the panels in Montreal that social networking can pose risks to the reputations of businesses. Companies may be responsible for improper disclosures, and whole institutions thrown into disrepute.

There was some discussion about online identity management. It was noted that many of the consequences of being social on the web could be mitigated if the technology enabled people to be more careful about their activities. One panelist commented that much

of the technological architecture online is "public by default, private by effort."[21] Others question why Louise is not getting more in return for giving up her personal information and, potentially, her reputation.

There was some discussion about how privacy needs to be built into systems and practices from the beginning, and what the default should be on the Internet. There was acknowledgement that fixing problems after practices have become entrenched can be costly for individuals and organizations.

Many participants noted that the behavioural advertising industry is still young and that technology is evolving rapidly. In some sense, in terms of privacy, organizations are trying to bring their privacy policies into line with their business practices. As a result, there are certain risks for individuals and organizations. For Louise, this typically means that her personal information is being gathered and used in ways that she may know nothing about. For businesses, it means that trust between organization and individual is being put at risk because of the invisibility of the practices and because the information can be misused.

OPC observations

The OPC agrees that traditional notions of public and private spaces are changing. Canadians continue to consider privacy to be important, but they also want to engage in the online world. The two are not mutually exclusive, but we think more needs to be done to protect privacy so that individuals like Louise can trust those offering her products, services and places to be social.

The OPC agrees that the practice of constructing profiles and drawing inferences based on social networking information that individuals post poses a range of risks to their privacy (and potentially other fundamental rights). Because individuals post online about themselves and their friends does not necessarily mean that they intend this information to be used by unseen entities to do with as they will. In our discussions in Montreal, it was noted that when people are on a social networking site, they tend to think they are among friends and are not acting as "consumers." The distinction between our social interactions and our "role" as consumers is disappearing. We are being turned into "always on" consumers.

It is still early days in terms of research into people's perceptions of their "invisible audience," and the possible disconnect between who they think their audience is and the reality. Complicating how people communicate and interact online, as researcher danah boyd notes, is that social networks, in particular, have certain properties that alter social dynamics: persistence, searchability, exact copyability and invisible audiences.[22] In terms of social networking activity, some early research suggests that individuals do make distinctions with respect to their intended audience and wish to exert some measure of control.[23] The difficulty in exerting control lies in the architecture of a site. When privacy controls are difficult to find or understand on a website, the ability of the individual to exert any control drops. If the site is popular and the individual is keen to be part of the community, he or she may risk being more open in order to participate in the site.

The OPC questions the view that since people put information "out there," it is therefore available for any kind of use. Some research is showing that people intentionally project specific personas online and post information that will support these personas, usually to gain some status.[24] It is not clear that the intention is always to be public. For example, someone may want to cultivate a professional presence online, but they may also want a separate social space to engage with friends outside of the work context. Making and keeping these worlds separate is neither obvious nor easy.

Moreover, in Canada, although personal information may appear in the public domain, this does not necessarily mean it can be used for any purpose. For example, PIPEDA provides that some publicly available personal information (as defined in PIPEDA's Regulations) can be collected, used and disclosed without an individual's consent; however, the purposes for which that information may be collected, used or disclosed are nonetheless limited.

The OPC is of the view that the consequences of the apparent breakdown between public and private lives can be seen most clearly in terms of harm to real-world reputations. Individuals—teachers, politicians, police officials—have lost jobs, been publicly embarrassed or lost benefits because of what they (or others) have posted online. On the Internet, data persists. Information that

harms an individual's reputation may never really go away. Moreover, with the increasing popularity of location-based applications, one consequence of telling people where you are is that you also tell them where you are not, potentially leaving your home at risk.

There are also implications with respect to the accuracy of the profiles data miners construct. Much has been made about the use of social network profiles in determining employability or acceptance to post-secondary education facilities. However, tracking and profiling online browsing behaviour also has consequences and is of great concern given the near invisibility of the practice. If these practices only resulted in targeted marketing, the risks of inaccuracy might seem minimal (although it could be problematic if people do not receive benefits that others do). If profiles are used more broadly—perhaps for granting loans, assessing insurance risks or assessing national security risks—the unforeseen consequences can be potentially more serious. There are also other potentially serious public policy issues that do not touch on privacy, such as limitations on freedom of speech.

The concept of "harm" appears to be used by some to distinguish certain practices that should require consent from those that should not. It should be noted, however, that PIPEDA does not contain such a concept. Rather, it requires that purposes be "appropriate," identified to the individual and consent obtained (the type of consent may vary). Instances where consent is not required are limited. Issues around consent are detailed later in this report.

The OPC has been following developments in the area of identity management as part of its strategic priorities.[25] Identity management may be helpful in providing individuals with better means of controlling their personal information, but it also has privacy implications in that, if it is not done well, data may be linked more easily to previously separate identities. We are interested in the ideas surrounding "digital identity" being proposed by Kim Cameron[26] and others. Digital identities should be flexible so that sometimes they correspond with natural, flesh-and-blood identities, and sometimes they are completely separate. These identities should allow someone to be public and private, according to the context. They should also allow the verification of a claim (e.g., old enough to drink) while adhering to a principle of minimal disclosure (e.g., not revealing the actual date of birth). We are tracking efforts to develop identity metasystems that allow for the effective creation and management of different identities.

The OPC supports the view that privacy considerations should be a critical component of the design stage of any technology or use of technology. In our recent submission to the Government of Canada on the Digital Economy Strategy, we noted that more could be done to prevent privacy problems or mitigate the effects on privacy protection posed by new technology by making privacy an integral part of the development of the digital economy. Other data protection authorities in other parts of Canada and the world are calling for "privacy by design" to be required in data protection legislation. The Information and Privacy Commissioner of Ontario, Ann Cavoukian, has been a longtime proponent of the concept of privacy by design.

The OPC is also of the view that privacy needs to become an integral part of the business processes and models that rely on technology through a careful analysis of companies' activities. Privacy impact assessments (PIAs) are a useful tool that the private sector should be encouraged to use since greater emphasis on such analysis may prevent problems from arising.

Expecting Louise and David to navigate the privacy implications of the many services and business practices online, to understand the implications and to consent to the practices may be unreasonable without a strong baseline of privacy protection. Knowledge and consent are key in PIPEDA, but there are other principles that organizations need to consider more carefully and build into technology and business models.

Issues for feedback proposed in the draft report – Public/private divide and reputations:

- The OPC would welcome further discussions with stakeholders on online identity management.
- The OPC challenges industry to find ways and means to help data expire and welcomes further discussions on this issue. PIPEDA is very clear that personal information should only be kept as long as it is needed.

Response to issues for feedback

Of the responses to the draft report that the OPC received, two referenced online identity management. One of these, from an advocacy organization, provided a number of comments. The organization asserted that anonymity is essential to privacy and referenced the pressures that prevent individuals from acting anonymously online. It referred to recent developments in which individuals are required or encouraged to display real life identities, such as in online news publications. In its view, heightened verification processes and the requirement to use real names on some social networking sites also erode online anonymity and therefore privacy.

However, one respondent to the draft report expressed skepticism that meaningful online identity management may be achieved through a combination of several approaches such as new technological tools and regulatory oversight. He suggested other approaches—namely, that the OPC have additional enforcement powers, such as order-making powers, including the ability to levy fines for non-compliance with PIPEDA. Outside of PIPEDA, he suggested that other legal tools be considered, such as private legal actions and a legal regime that imposes liability on online social networks for harm created by only privacy breaches (similar to the copyright liability regime that is in place in the U.S.).

PROPOSED ACTIONS:

- The OPC will continue to monitor and fund research developments on the implications of changing perceptions of public and private spaces (as well as the challenges of maintaining a professional and personal presence online), through our Contributions Program.
- The OPC will conduct public opinion research on Canadians' perceptions of the public-private divide.[27]
- The OPC will conduct outreach activities, including developing best practices for organizations to support people's capacity to be as private—or as public—as they want.
- The OPC will continue our public education efforts focused on Canadians.
- The OPC will work with Industry Canada to consider how best to integrate privacy by design principles and PIAs into private sector practices.
- The OPC will monitor and draw on, where possible, the work of our international colleagues who are working on these issues.

WHAT WE HEARD

Children need special attention

During the consultations, we heard about how the public/private divide is even more acute for children, who are using the Internet at younger ages and are providing their personal information to websites with little clear notion of how the information will be used and why. Children like David are largely playing on commercial sites, where there appears to be a blend of entertainment and "infotainment" in which the games that children engage in, for example, are a means for gleaning information about those children—how they play, what they like, how they think. Many of these sites are not only collecting children's information; as in Louise and David's case, David relies on Louise's credit card information to sign up for games and, in so doing, the site is collecting both his information and hers. Some sites also ask children to disclose information about their parents.

Many noted that there is a serious lack of transparency in how personal information is collected or used, so that if parents wanted to find out more about the site's privacy practices, they may find it difficult. Also discussed was children's perception of privacy. Children think they are only "talking" to friends; they are not aware of the "invisible audience." They are of the view that if adults have seen their information or used it in some way that the child thinks is wrong, it is the adult who is in the wrong and should be the one to take corrective measures. It was also noted that children under a certain age have no sense of marketing. They do not know when they are being advertised to and when they are not. This is significant given that the age of children active online is dropping. One participant in the children's panel called for a law against the exploitation of children for profit. During the discussions, the CMA referred to its guidelines with respect to children's advertising. However, one panelist remarked that many online practices are not in keeping with those guidelines.

OPC observations

The OPC shares the serious concerns raised with respect to children online. An amendment[28] to PIPEDA is currently being proposed that may help address concerns about some of the privacy practices of certain websites aimed at children. Though not specific to children, it would require that the consent be considered valid only if it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure of personal information to which they are consenting. PIPEDA already requires meaningful consent, and such an amendment is expected to enhance and clarify this requirement. We support the proposed amendment to PIPEDA and welcome this clarification.

In keeping with our position on how technology and services are developed, the OPC is of the view that baseline standards need to be developed to support parents and educators in terms of knowing that children's personal information is being protected. A framework needs to be put in place that will better inform parents and educators and, ultimately, will better protect the personal information of children such as David. While we note that marketers are bound by certain guidelines concerning children's advertising, behavioural advertising is not included in those guidelines.

Issues for feedback proposed in the draft report – Children need special attention:

- The OPC welcomes comments on what baseline standards regarding children's personal information should be and how they can be developed. We also welcome views on what kind of framework should be put in place.

Response to issues for feedback

The OPC received no specific feedback on what the baseline standards for protecting children's personal information should be and how they can be developed, or on what kind of framework should be put in place. We did receive information on what one company is doing for children online. This company also noted some of the challenges around behavioural advertising and children. Also, one association offered to work with the OPC on children's issues and the public/private divide.

This is an area that the OPC will continue to explore in the future.

WHAT WE HEARD

Digital citizenship is key

Some respondents commented that everyone—users of all ages, businesses and regulators—needs to be better educated about how their online and offline activities can affect their lives. There was general agreement that more work needs to be done to better inform users about online privacy, and that we need to find innovative and creative ways to do so.

OPC observations

The OPC agrees with this position and is of the view that privacy should be part of a digital citizenship program, to ensure that individuals participating in the online environment function in a way that is respectful of their rights, values and ethics, and supports constructive interaction and trust. We agree that better, more effective ways of reaching out to individuals to help them understand the consequences of their actions are needed. In our own work with youth, we have seen a great interest in and demand for educational tools and resources.

As we noted, however, in our submission to the Government of Canada's consultations on Canada's digital strategy, youth should not be the only focus. Developers, business leaders and users of all ages need to have a solid grounding in privacy principles if we are to protect Canada's online marketplace.

PROPOSED ACTIONS:

- The OPC will work on focusing our online privacy activities on adult Canadians who may be newer users in the online environment.
- The OPC will continue our dialogue with the technical community on how to build the principles contained in PIPEDA into both the user interfaces and underlying technology.
- As part of the OPC's public education activities, we will continue to reach out to youth and will continue to seek innovative and creative ways of doing so. The OPC will continue to seek ways to work with our provincial and territorial counterparts on such activities.

II.V PIPEDA – Privacy principles

During the consultations, we found that the biggest challenges to the privacy principles laid out in PIPEDA for industry, individuals and the OPC appear to arise from the practices of online tracking, profiling and targeting. Defining personal information, determining the appropriate types of consent, ensuring control over one's personal information—these are core issues that require attention if we want to provide better privacy protection for Canadians of all ages.

WHAT WE HEARD

PIPEDA – flexible and neutral

Many of those who made submissions or participated in our consultation events noted that the strengths of PIPEDA are that it is technology neutral and principle based, and therefore flexible. This is a position that our Office has shared and continues to share. So far, PIPEDA has been a dynamic, effective instrument that has strengthened the privacy rights of Canadians.

However, not all respondents and participants share the view that PIPEDA is up to the task. There are some issues relating to the scope of privacy protection, as well as the fair information principles at the core of PIPEDA, that we identified from the submissions and participation in the events that merit careful study and consideration. These are discussed further below.

Definition of personal information

Determining whether the data being collected, used or disclosed is personal information is a fundamental step in defining the scope of the application of PIPEDA in the circumstances.

We noted that there was some disagreement in terms of how various respondents described the information being collected when individuals' online activity is tracked.

- Two of the 21 written submissions (one of which was from an association) either drew a distinction between "data collected through advertising" or "non-identifying information," and "personal information" or "personally identifiable information."
- One (another association) questioned whether browsing data and an IP address qualified as personal information.
- One respondent stated that it engaged in "interest-based" advertising, but that this practice did not include the collection, use or disclosure of personal information.
- Another submission noted the distinction that many online companies made, often using "personally identifiable information," when in Canada, the term is "personal information."
- The variations in terminology were reflected in the panel discussions at the consultation events. "Confidential" information was used during one of the panels, its meaning apparently similar to that of "personally identifiable information."

Apart from the discrepancy around the terminology, it appeared that many respondents and participants (though not all) agreed that online tracking, profiling and targeting implicates privacy.

OPC observations

Personal information, as currently defined in PIPEDA, is "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization."

PIPEDA does not contain any definition for "personally identifiable information," "non-identifying information" or "confidential information." The term "personally identifiable information" is one that is used in other jurisdictions and typically refers to a narrow set of information that can be used to uniquely identify an individual. Examples include an individual's name, address, national identification number or driver's licence number. By contrast, the concept of personal information as set out in PIPEDA has been interpreted by the courts and the OPC to apply more broadly.

In 2008, the OPC issued an "Interpretation" document that outlined general interpretations by the courts of the term personal information, as well as summarized the position we have taken in various PIPEDA-related complaints where the question of personal information was debated.

The OPC has generally taken a broad and contextual approach in determining whether certain information is or is not personal information. Of note is a finding from 2003, in which it was concluded that the information stored by temporary and permanent cookies was personal information.[29] The Office has also determined that an IP address is personal information if it can be associated with an identifiable individual.[30]

Other noteworthy examples include an investigation into the collection and use of GPS information placed in a company's vehicles, in which it was concluded that such information is personal information since it could be linked to specific employees driving the vehicles. It was noted that the employees were identifiable even if they are not identified at all times to all users of the system.[31] Information collected through radio frequency identification tags (RFID) to track and locate baggage, retail products and individual purchases may constitute the personal information of any identifiable individual associated with those items.[32]

What does this mean for the data collected through online tracking?

The OPC is concerned about the variance in terminology used in the submissions and discussions. There seems to be an attempt to stress that the information collected is anonymous ("non-identifying" or "non-confidential") presumably because it does not contain information that identifies the individual by name (referred to by some respondents as "personally identifiable information").

However, true anonymity is becoming a more difficult state to achieve, given the advances in technology.

Some respondents would like the OPC to provide guidance on determining the point at which tracking information becomes information about an identifiable individual. Without conducting an investigation, it would not be prudent for the Office to definitively state that all online data collected is or is not personal information. In certain cases, we have determined that IP addresses, for example, are personal information, including in the context where an IP address is associated with an individual's online activities. We have also found that cookies are personal information. While we realize that there are grey areas and that context will always be a factor, the above examples of OPC findings illustrate that the information involved in online tracking, profiling and targeting has been found to be personal information in the past—a point that organizations may want to consider when developing their practices.

We note that the FTC has taken a broad approach in its Self-Regulatory Principles for Online Behavioral Advertising, applying the scope to not only "personally identifiable information" but also to "non-personally identifiable information," noting that "the traditional notion of what constitutes PII versus non-PII is becoming less and less meaningful and should not, by itself, determine the protections provided for consumer data." It goes on to note that "the Commission and other stakeholders have long recognized that both PII and non-PII raise privacy issues."[33] In December 2010, in its proposed framework for protecting privacy, the FTC advocates applying the framework to data that can reasonably be linked to a specific consumer, computer or device.[34] With respect to behavioural advertising, the European Union Article 29 Working Party issued an opinion on the practice, noting that the methods (used in behavioural advertising) often "entail the processing of personal data as defined by Article 2 of Directive 95/46/EC."[35]

We therefore think that the contextual approach to defining personal information that the OPC has used in the past will not be at odds with the views of international regulators on the subject.

PROPOSED ACTION:

- The OPC has updated and will continue to update where necessary our Interpretation document with respect to personal information.

Consent, meaningful consent and transparency

We heard much discussion about the appropriate type of consent for online tracking, profiling and targeting, and nearly everyone agreed that transparency is vital to the practice. For the most part, the industry associations and businesses were generally in favour of "opt-out" consent with respect to behavioural advertising, with one stating it should be "opt-in" where the information is sensitive. Another association, however, preferred opt-in consent for behavioural advertising regardless of the sensitivity of the information.

Many of the associations noted that self-regulatory measures are being taken to address the transparency issue. Conspicuous links by ad networks and websites about advertising practices were cited as potential strategies to deal with the consent issue. We heard about different ways that transparency (and opt-out) could be achieved through a special icon (the "i" icon) that an individual can click on and be provided with immediate information.[36] We also heard about various education initiatives, including a site that provides individuals with information on protecting their privacy online. Some websites are starting to give users the opportunity to manage the interests that a "publisher" or ad network has associated with their browsing habits. There was general agreement that individuals should not have to search for information. There was also agreement that information needs to be easy to understand yet sufficiently detailed, though it was also noted that the practice itself is fairly complex and would be difficult to explain.

Those more critical of the practices questioned whether the requirement under PIPEDA for consent to be meaningful was being met since there was often a lack of

detail in descriptions of practices—where information was provided at all. One individual questioned whether all the information being collected was necessary for the purpose of serving advertisements.

OPC observations

If it is challenging to determine whether data is or is not personal information, the issue of consent is equally complex. We note the work many industry associations are doing to incorporate transparency and the other fair information practices into their best practices guidance to members. The following is an overview of how the OPC has addressed the issues of consent, meaningful consent and transparency in the past, and what some of the challenges to consent presented by online tracking, profiling and targeting might be.

What has the OPC said in the past about consent?

In 2004, the OPC issued a fact sheet on consent that largely remains our interpretation of the knowledge and consent requirements in PIPEDA. We have applied this reasoning to various types of practices and have considered the appropriate type of consent in various contexts.

PIPEDA states that the knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate. The Act goes on to note that the type of consent may vary depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (e.g., medical records and income records) is almost always considered to be sensitive, any information can be sensitive depending on the context. It does note that express consent should be sought when the information is likely to be considered sensitive, while implied consent is generally appropriate when the information is less sensitive. Finally, the Act notes that in obtaining consent, the reasonable expectations of the individual are also relevant.

The OPC's view has always been that "opt-in" (express) consent is the preferred method of consent although "opt-out" may be acceptable under certain circumstances.

What is opt-out?

For example, an organization presents an individual such as Louise with an opportunity to express non-agreement to an identified purpose. Unless she takes action to "opt out" of the purpose—that is, to say "no" to it—the organization assumes consent and proceeds. Louise should be clearly informed that the failure to opt out will mean that she is consenting to the proposed use or disclosure of the information.

The OPC has had opportunity to consider the use of opt-out in a number of different contexts. A common use of opt-out is in the context of using or disclosing personal information for secondary purposes of marketing. Secondary purposes are additional to those for which the information needed to be collected in the first place. The Office considers that an organization must satisfy the following requirements when using opt-out, for example, to obtain consent for secondary marketing purposes:

- The personal information must be demonstrably non-sensitive in nature and context.
- The information-sharing situation must be limited and well-defined as to the nature of the personal information to be used or disclosed and the extent of the intended use or disclosure.
- The organization's purposes must be limited and well-defined, and stated in a clear and understandable manner.

- As a general rule, organizations should obtain consent for the use or disclosure at the time of collection.
- The organization must establish a convenient procedure for opting out of, or withdrawing consent to, secondary purposes. The opt-out should take effect immediately and prior to any use or disclosure of personal information for the proposed new purposes.[38]

Our position on opt-in versus opt-out consent and the criteria we developed, particularly with respect to marketing, grew from our experiences with traditional bricks-and-mortar organizations. It evolved somewhat with our examination of a social networking site's use of user personal information for advertising.[39] In that instance, we took into consideration the role that advertising plays in the business model of such a site, as well as what may or may not be considered sensitive within that context.

Online tracking, profiling and targeting is a highly complex environment in which to consider the appropriate type of consent. To begin, the ways in which data are collected, and the uses to which that data are put, are largely invisible to most users—and certainly more so to children. There are more players (e.g., websites, ad networks, data miners) involved, and the user may not know who these players are. Even a user like Louise, who is fairly savvy about online tracking practices, will not likely know who is collecting her data. If she is curious about the types of information being collected about her and the kind of profile she is being given, it would likely be difficult for her to find out who holds what information about her. The question of accountability, as well as accuracy and access, will be addressed later in the report.

Transparency and meaningfulness of consent are serious issues and they generated a great deal of discussion on the panels. It is perhaps easy to get lost in the issue of opt-in versus opt-out, but one issue that needs serious consideration is that of *meaningfulness*. Are the purposes and practices clear so that the consumer is giving meaningful consent? This is a question of fairness, as well as a requirement under the law—and it is one area that we think needs more focus.

PIPEDA talks about organizations being open about their policies and practices. Information provided to consumers about online tracking and targeting are often overly complex or legalistic. Individuals are often not interested in paying attention to privacy notices, which often adopt a "take it or leave it" approach. Even if they are well written and easy to understand, are there ways in which people could be encouraged to read through them? We heard about some positive developments in terms of better informing consumers about online tracking, profiling and behavioural advertising. There was discussion on the panels about the "i" icon, to be added to most online ads that use behavioural data, which informs consumers of behavioural advertising and what happens when they visit a specific website. Better written, more easily accessible privacy policies were also discussed—layered notices, privacy "nutrition" labels—are some examples of work that could offer better information to consumers. The challenges of obtaining meaningful consent are exacerbated in the mobile world. The screen is small and it is difficult to provide users with the detail needed.

PIPEDA also requires that the purposes for collecting, using and disclosing personal information be identified, typically at the time of collection. In the case of behavioural advertising, if information is provided next to the ad, it comes after the information has already been collected and used in some fashion. While we are encouraged by innovative ways to better inform individuals, and we think the "i" icon is a step in the right direction, opt-out consent may not sit well with many users. However, some will say that it interrupts the user experience to ask for consent each time the user logs on.

There was some discussion during the consultations about cookies—users can take the action of blocking cookies or deleting them and then opting out of ads by clicking on the ads (provided they allow a user to opt out of them). There are limits, however, to the effectiveness of relying on cookies, and relying on individuals' abilities to navigate the privacy tools available to them. Flash cookies, for example, are not usually visible to users, and options to control or delete them are usually absent or very difficult to find. Flash cookies can be used to recreate web cookies

if the latter are deleted. Super cookies are often invisible to the user, who is often not provided with tools to control the information that is stored. Some tools are available on browsers for users to control the collection of their surfing activities, but these have limitations, in that they generally delete some types of cookies but not others. In order to clear all the different forms of cookies and web storage, users would have to install and use special add-on applications. Is this reasonable to expect of the average user? And would the average user reasonably expect to have to take such measures just to prevent tracking and profiling? One industry association talked about providing a one-click access to information about behavioural advertising, with the opportunity to opt out of behavioural advertising (using a permanent cookie). Provided it works as anticipated and is broadly implemented, such a development could help address some of the concerns about ease for users.

In considering the appropriate type of consent, there is also the question of sensitivity. There are some grey areas with respect to sensitive personal information. What is sensitive for some may not be for others, and what could be considered sensitive in one context may not be in another. The problem with trying to assess sensitivity online is that the environment lacks context.

Some commentators say that privacy could be better protected if the focus were placed on the use of the information. Is that use harmful to the individual or not? Not all uses are harmful: many might agree that being served advertisements tailored to interests does not impinge on dignity, but online activities being used to assess your creditworthiness might. The concept of harm, however, does not exist in PIPEDA. Rather, it centres on the collection, use or disclosure of personal information for appropriate purposes. Informing and obtaining consent of the individual to such purposes is required. Focusing solely on the end use also ignores the sense that many have of not liking the idea of being "followed" once they log on.

Is there a practical approach to assessing sensitivity and determining the appropriate form of consent?

Some companies already limit their tracking and do not use certain information that is generally considered sensitive (e.g., health information). The OPC thinks this is a useful, practical approach.

We also heard discussion about a Do Not Track registry. This is an idea that is gaining support in the United States and is of interest to us. In the FTC's December 2010 proposed framework, it endorses a Do Not Track mechanism.[40] In one of the responses to our draft paper, an advocacy organization expressed its support for a browser-based mechanism by which users can monitor and, if they choose, prevent online tracking. The organization echoes the FTC's proposed framework, which calls for a simple mechanism that consumers can use to indicate their intention not to be tracked. As indicated in the FTC paper, such a mechanism should provide granularity so that users could opt in to specific advertising networks while blocking others. According to the organization responding to our draft paper, such a mechanism must also prevent collection of user browsing, and there should be strong penalties for non-compliance.

A Do Not Track mechanism offers a practical means for individuals to protect their browsing activities, but there are jurisdictional and technical issues associated with it. It would also require a reasonable understanding on the part of individuals of how tracking takes place and what the information is used for, not to mention taking an active action on their part to remove themselves.

A proposed amendment to PIPEDA would require that the consent be considered valid only if it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure of personal information to which they are consenting. This amendment may enhance and clarify the requirement for meaningful consent and may help address some of the concerns about tracking, profiling and targeting children, particularly those who are not yet at a stage

in their development where they can understand how and why their information is being collected and used. The appropriateness of relying on opt-out consent with respect to the tracking and targeting of children would be even further in question. The OPC also notes, however, the comments in one of the responses we received on the draft report. The company providing the response indicated that there are challenges with respect to behavioural advertising and children, in terms of knowing the age of the individual who is browsing online. It stated that websites and advertisers presenting marketing on those sites will not be able to tell whether visitors are adults or minors without age restrictions or authentication mechanisms in place.

Interestingly, in terms of location services, as we understand it, the Canadian mobile advertising community appears to be cognizant of Canadians' concerns about others knowing where they are and their wariness about being served advertisements based on location. They noted the "intimacy" of the personal device (i.e., a mobile phone), and commented that they ask users to opt in to being served advertisements based on location. We see this as a positive and appropriate approach.

Appropriate purposes

At least one of the respondents commented on whether tracking was appropriate at all. This perspective was also echoed in one of the responses to the draft report. This is an important consideration. PIPEDA contains a clause that states that organizations may collect, use or disclose personal information for a purpose that a reasonable person would consider appropriate in the circumstances.[41] We will not offer our view on whether profiling and targeting, per se, are appropriate, but we would stress that this provision is one that business needs to consider carefully, particularly in light of the discomfort many individuals express over tracking, profiling and targeting. They may appreciate some of the services they receive, but this does not obviate the need to inform individuals and allow them to make their own decisions about what they do and do not want.

Issues for feedback proposed in the draft report – Consent, meaningful consent and transparency:

- The OPC will continue to work with industry to develop the best approach to ensure that individuals are providing meaningful consent to legitimate business practices. This may be an area in which technology can prove helpful in addressing this problem. In that regard, we would welcome comments on how best to achieve this.
- The OPC will continue to focus our outreach activities on individuals to help them better protect themselves online. This will include exploring how best to help individuals focus on privacy explanations that are provided to them. The OPC welcomes any comments on how best to achieve this.

Response to issues for feedback

In the feedback we received to the draft report, industry representatives reiterated their view that opt-out consent is appropriate and that transparency and consumer participation need further work. One academic noted that consent has been overemphasized in the past, at the expense of other principles, most notably the collection limitation principle. He suggested that if more focus is placed on limiting the amount and type of personal information collected, consent might become more meaningful.

An advocacy organization took the position that the form of consent is a critical element in determining whether consent is meaningful. Countering industry's position that requiring users to take certain steps before giving consent would interfere with the users' experience, the organization stated that requiring individuals to opt out of features, services or settings that a user thinks insufficient from a privacy perspective is as disruptive of user experience, especially since many opt-out mechanisms are difficult to find and understand.

The organization is of the view that transparency is necessary, but it is not sufficient in an online environment, and that organizations have the opportunity to develop "creative consent mechanisms" to ensure that users are agreeing to online practices.

PROPOSED ACTIONS:

- The OPC will conduct or support research on innovations in privacy explanations and will examine the merits of promoting certain types of privacy explanations.
- The OPC will continue to seek ways, with our provincial and territorial colleagues, to help inform parents of the need to protect their family's personal information online.

Other uses and disclosures

Although the majority of the written submissions that we received concerned behavioural advertising, there was some discussion on the panels about what other uses of profile information might exist, and the lack of control some believe users like Louise have over their personal information. There was concern expressed about some of the uses that people are aware of—using social network data to conduct psychological assessments, to assess creditworthiness or for law enforcement purposes, to name a few examples. Generally, the concern was that tracking and profiling individuals to serve relevant advertising is one thing, but using such data or social networking information for other unknown purposes was disconcerting. A fear was expressed by some that since the practices are largely invisible to users, the ability to store data indefinitely exists, and the technology to process the data for new uses is ever-improving, the potential for other uses may be very attractive. Data could also be sold and individuals might never know about it. However, some industry representatives stressed that there are requirements under PIPEDA to request consent for new uses of information, and that the law provides protection for individuals and recourse in the event of misuse.

Some noted that, as a society, we should be concerned about the amount of data being collected by large corporations. During some of the discussions, it was noted that the laws are "disturbingly permissive" when it comes to the flow of information from private companies, which seem to know more about us than we know about ourselves, to law enforcement. The point was made that law enforcement authorities are required to obtain a warrant to access information about us and the information they are obtaining is becoming richer. At the same time, laws are permitting private businesses to share information with the police without a warrant or our knowledge or consent.

OPC observations

Although we received 21 written submissions, we would have liked to have heard from a broader range of organizations. We would have benefitted from their views on behavioural advertising, as well as on some of the other uses of profiling information.

We are aware that in the United States profiles built from individuals' social media activities are being used not only to target consumers to offer them new products and services, but also to make lending decisions.[42] The process is termed Social Media Monitoring (SMM) and uses information on social networking sites like Facebook and Twitter, comments posted on sites like Amazon, reviews on sites such as Yelp or blog posts to populate social graphs. Along with a growing trend toward relationship marketing and research that shows the influence friends have on purchasing decisions, data miners have made the assumption that information about your friends' behaviour can be used to better predict your behaviour—other people's personal information is becoming your personal information and, without your consent or knowledge, will impact decisions made about you.[43]

It has been noted that when people post where they are through location-based services, they are also posting where they are not. Some have speculated that the insurance industry could increase premiums or deny claims of clients if they are users of location-based services such as Loopt and Foursquare that share their current location.

Apart from general discussion on the panels, there was little information about the extent of such uses of social data in Canada. How else is such information being used in Canada? What about the mixing of information in offline databases, such as that collected through loyalty cards and

online coupons for real-world stores? We did not get a full picture of even the behavioural advertising ecosystem.[44] We are concerned that we are missing important aspects of that practice, not to mention other practices that were not discussed in depth on the panels, such as online gaming. The OPC is of the view that, in the interest of Canadians, there needs to be public discussion about the status of certain practices, where they might go and whether this is something the public wants.

The OPC agrees that user control over personal information is vital. We are of the view that with greater visibility of practices and clearer consent provisions, users like Louise will have improved control. We are also of the view that improved architecture may also provide better baseline protections. We agree with the panelist who noted that PIPEDA requires additional consent to any new use of personal information. However, relying solely on complaints to be brought to us in such an event may leave questionable practices unchecked.

Some respondents also suggested that the OPC focus our attention on the use of online tracking and profiling by government. We are aware of the possible uses of such information for government purposes.

Issues for feedback proposed in the draft report – Other uses and disclosures:

- The OPC welcomes additional views and comments regarding current and future online tracking and profiling practices (other than behavioural advertising) in Canada.

Response to issues for feedback

An advocacy organization provided comments on various types of tracking. With respect to tracking that is considered necessary to improve services or products, it noted that some of the activities that fall into this category can be quite broad—from predicting product preferences to perfecting search algorithms to recommending potential friends to people on social networking sites. Some of this may involve tracking the individuals' actions on the website itself and/or the individuals' activities across other sites and retaining such data. Though noting that some of these activities may be "legitimate," the organization was of the view that they are often broad and invisible to users.

The organization also commented on the potential for much user-generated data to fall within the journalistic purposes exception under PIPEDA. It is of the view that amendments may be needed to this exception to narrow the scope to incorporate a reasonableness criterion, in order to balance the level of intrusiveness of the information being disclosed and the importance of the information in question. It expressed concern about the lack of protection for privacy invasions that may occur online outside the scope of commercial activity. The organization flagged this as an area that needs further exploration to find solutions to the privacy risks posed by individuals' capacity to potentially affect others' privacy. Such examples may include situations where consent is sought not directly from the individual by a "friend," for example through tagging practices, posting photographs or adding applications in which other people's personal information is disclosed.

The organization referred to our findings in the 2009 Facebook investigation report and our comments on the need for individuals to obtain the consent of others before engaging in some of these practices (our comments specifically referred to the provision of e-mail addresses of non-members in order to invite them to join Facebook). It stated that where it is impossible for the individual to obtain consent, then reasonableness should be applied. It noted, however, that there may be times when it is reasonable to imply consent to some disclosures but not to others. The organization is particularly concerned about the situations where such sensitive information as location is recorded in searchable form or transformed into metadata made available to developers.

In another response to the draft report, the writer took the position that the OPC has interpreted commercial activity too narrowly—namely, that information posted by individuals about other individuals on social networking sites is part of the socializing that occurs and is not part of the commercial activity conducted by the site operators. The writer argued that behavioural advertising depends on the amount of personal information on these sites (and the Internet). If the OPC were to consider personal information collected in the course of a commercial activity as including all of the personal information held by an organization, more of the organization's practices would fall

under PIPEDA. This perspective is an interesting one; we are aware of this view, but have not had the opportunity to fully examine it and its implications.

PROPOSED ACTIONS:

- The OPC urges industry associations to continue working with their members to remind them that consent to new uses is an integral part of privacy protection under PIPEDA. We will express our views to the associations, as appropriate.
- With respect to government uses of online information, the OPC will continue to monitor developments in this area and express any concerns we may have with the appropriate parties.

Safeguards and retention

Closely tied to the concerns expressed in secondary uses of personal information were those related to safeguards and retention. Those expressing apprehension about secondary uses of personal information noted security issues and the ability to store data indefinitely as factors that may contribute to misuse or to expanding uses. The industry associations recognize the importance of safeguards and retention, and the self-regulatory models that many of them have put into place include the requirements to ensure data security and limit retention.

We also heard during the panel discussions about how data can live on in the digital environment, that it is cheaper to store data than to get rid of it, and that there may be potential uses of the data that are very attractive. Some noted that deleting data online is more difficult (if not impossible) to achieve. In the responses to the draft report, two companies noted that more work should be done on establishing data retention standards.

OPC observations

The OPC agrees that safeguards and retention are important issues and we are pleased that industry has included these in their self-regulatory models as they are also contained in PIPEDA, to which their members must adhere. The more the self-regulatory models resemble the laws that companies operating internationally need to abide by, the easier it will be for organizations to be reasonably sure that their practices meet various regulatory requirements in other countries.

Cyber security is a serious and growing concern. There are a number of factors contributing to this problem, including more electronic data being stored and processed; ever-increasing complexity of computer hardware and software; and ubiquitous computing devices that are often portable (smart phones, PDAs, laptops). The OPC is pleased that the Government of Canada has introduced amendments to PIPEDA to make breach reporting mandatory as this has the potential to strengthen security requirements.

We agree with the concern about the implications on reputations and possible misuses as a result of data living on indefinitely. We also recognize that this is an issue which requires technical solutions to fulfill policy and legislative requirements to not keep personal information indefinitely. This issue was also discussed in the section on the public/private divide and reputations above.

PROPOSED ACTIONS:

- The OPC encourages industry to develop technical approaches to addressing retention issues.
- The OPC encourages the CRTC to develop benchmark privacy guidance that meshes existing regulation of broadcast/online advertising with protections for confidential consumer information.
- The OPC is working with Industry Canada to develop guidance on data disposal.

Access and correction, accuracy of information

The concerns expressed about reputation are linked to issues around accessing one's own personal information and having the ability to correct it. However, many noted that individuals often have difficulty finding out who has their personal information (beyond those places to which they have given their information directly), how it is used and how they can have errors corrected. Compounding this is the fact that information is often held in another country (this is expanded on in the section on cloud computing below). Given that tracking and profiling is largely invisible to most users, they likely have no idea what is going on and therefore have little control over how their information is being collected, used or disclosed.

We heard about some innovative developments by certain entities that provide a variety of web-based services to let users such as Louise know what information is being held about them, and to let them choose what categories of advertisements they want (or to opt out of receiving advertisements altogether). Some concerns were expressed about the risk that inaccurate data may be used to make decisions about individuals, with varying consequences depending on how the data are used.

OPC observations

The OPC agrees that the ability to access and correct one's own personal information plays a key role in controlling one's personal information. We recognize that access and correction may be more challenging for both individuals and organizations given the online environment and how personal information is defined. Nevertheless, we are of the view that technology may be able to provide some answers on how to meet these requirements under PIPEDA.

PROPOSED ACTION:

- The OPC encourages industry to find innovative ways to meet the access/correction and accuracy provisions that meet PIPEDA requirements.

Accountability

Underscoring all of these issues is the question of accountability. The industry associations that provided written submissions acknowledged that this must be addressed. Who is doing the tracking? Where do individuals go to review their profiles and make corrections? Who is safeguarding their personal information? Who do they talk to about withdrawing consent? Who will handle their concerns if they have a complaint? Some work is being done in this area to increase the visibility of the practices and to offer individuals more information about online tracking, profiling and targeting.

OPC observations

The OPC agrees that accountability is key to ensuring that the personal information of users such as Louise and David is not misused, that they are informed, and that they have given meaningful consent to how their personal information is collected and used.

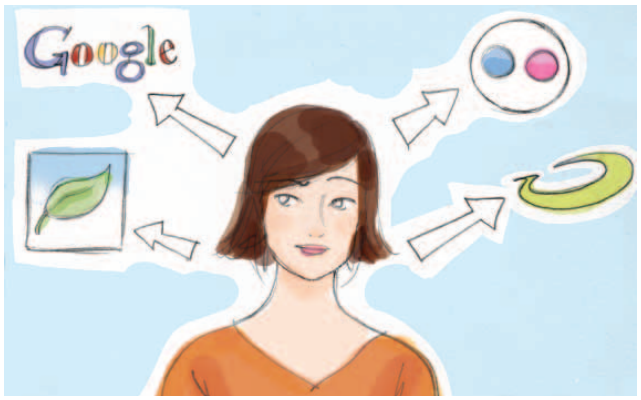
We recognize the steps that industry associations and some organizations are taking steps to be accountable for any online tracking, profiling or targeting that they or their members engage in, and we encourage them to continue focusing on this important component of privacy protection.

CLOUD COMPUTING

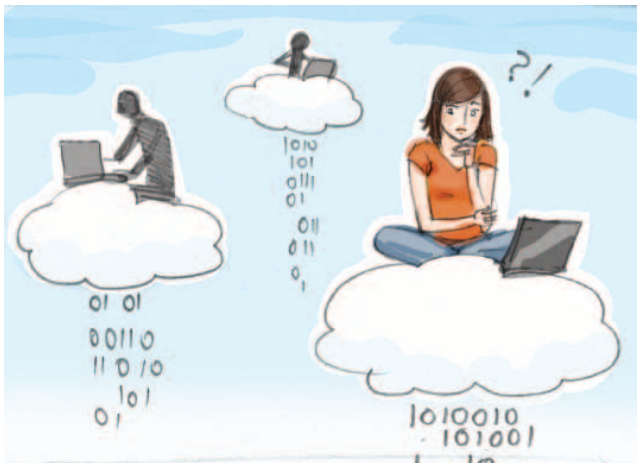
Louise's jewellery business has been doing well, and she has expanded her client list and her product line. As her small business grows, Louise realizes that she needs to start handling her electronic documents more professionally. However, she is not a computer expert and has limited time to spend on technical details. Louise thinks she needs some help to manage her data effectively. She has been hearing a lot about the advantages of cloud computing, and wonders if this might provide her with some useful business tools.

Louise already uses a Gmail account for her business communications, and she uses Flickr to store photos of her jewellery creations. She accesses her business bank account over the Web through online banking. She is considering using a cloud address book application to keep track of her growing list of

clients and suppliers. She is also looking at FreshBooks for online expense tracking and invoicing.



Although Louise is interested in using these cloud services, she has some concerns about taking the leap into this new model. Louise is not entirely sure about the technology underlying cloud computing, and how the business models work. There are also a lot of unfamiliar terms, like "virtualization," which can be hard for a non-expert to understand. She also wonders how service providers will manage, use and protect her information. She worries whether she will be able to get access to her data whenever she needs it, and whether it will be safe from hackers and bad software. Louise is concerned about where her information will be stored—she has heard that it might be in another country, and wonders what legal implications that might have for both her business and personal data.



III.I What is cloud computing?

Cloud computing is defined in many different ways. In general, it is the provision of web-based services, located on remote computers, that allow individuals and businesses to use software and hardware managed by third parties. Examples of these services include online file storage, social networking sites, webmail and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

When it comes to cloud computing, Louise plays various roles. As we saw in the first section of this report, Louise is an avid user of social networking sites. But Louise is also an entrepreneur, and as such, she uses cloud services such as Gmail and Flickr for some aspects of her business. She is now considering using certain cloud services to help her handle her customer accounts. In each situation, her expectations and her role, in terms of privacy protection, change. When she is a social network user, she is interacting directly with the service as an individual. To the extent that the service has a real and substantial connection to Canada, and collects, uses or discloses her personal information in the course of a commercial activity, she is protected under PIPEDA, and the organization is required to put in place certain practices that are in compliance with the law. With respect to her jewellery business, Louise is engaged in a commercial activity and is handling personal information. She is therefore required to be accountable for the personal information she entrusts to a cloud provider.

Whether it is Louise's personal information in the cloud or whether it is her clients', there are challenges around protecting personal information. The following is an overview of what we learned from the submissions and panel discussion in Calgary, our observations, issues we would like feedback on, and some proposed actions.

III.II What we learned

Many of the 11 written submissions we received and the discussions at the public event in Calgary provided detailed and useful explanations of cloud computing and cloud computing models. Of the 12 responses to the draft version of the report, three commented solely on cloud computing, while two others commented on cloud as well as on online tracking, profiling and targeting.

The definition developed by the U.S. National Institute of Standards and Technology (NIST) was cited by a number of respondents and bears repeating in this report:

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.[45]

These characteristics include on-demand self service, broad network access, resource pooling, rapid elasticity and measured service. The service models are software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS). Cloud services are typically deployed via a private cloud, community cloud, public cloud or hybrid cloud. These characteristics, service and deployment models are described in more detail in the NIST definition.[46]

One respondent stressed the differences between public and private clouds as these may have different privacy implications. According to the NIST definition, in a public cloud, "the cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services."[47] Public clouds offer resources over the Internet. Examples of public clouds include services aimed at consumers, such as online photo storage services, e-mail providers or social networking sites, as well as services for enterprises. In a private

cloud, "the cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise."[48] Whether an organization uses a public or private cloud, the organization (including Louise when selling her jewellery) that makes arrangements with the cloud provider would be responsible for protecting personal information and for ensuring the cloud provider that processes the personal information provides a comparable level of protection, as required under PIPEDA.

A distinction was also drawn in some of the written submissions between "consumer services" and "enterprise services." One respondent noted that where the cloud service is offered directly to consumers, the provider is the data controller[49]; however, where the services are offered to enterprise customers, the provider is the data processor. Generally speaking, in Louise's case, when she uses her social networking site or e-mail for fun, the social networking site or e-mail provider is the data controller. When she wishes to use a cloud service to help her handle her jewellery customer data, the provider is a data processor and Louise is the data controller. This distinction is important because it means that when Louise is the data controller, she has certain obligations to her customers in terms of privacy protection.

Benefits and risks

Some of the respondents and participants noted the benefits that cloud computing provides. Some of the benefits to users (businesses, especially small and medium-sized enterprises, governments and individuals) include scalability (offers unlimited processing and storage capacity), reliability (eliminates the concern of losing valuable data in paper format or via the loss of laptops or hard drives; enables access to applications and documents anywhere in the world via the Internet), cost savings, efficiency (frees up resources to focus on innovation and product development) and access to new technologies. Some respondents and participants noted that since cloud users do not have to invest in information technology infrastructure, purchase hardware or buy software licences, the benefits are low up-front costs, rapid return on investment, rapid deployment, customization, flexible use and Internet scale solutions that can make use of new web-based innovations. Some noted the potential benefits to society such as better delivery of health care, economic growth and job creation.

One potential benefit cited by a number of respondents and participants was that privacy may be improved. Specifically, cloud computing may improve privacy by design efforts and the use of better security mechanisms. It was noted that cloud computing will enable more flexible IT acquisition and improvements, which may permit adjustments to procedures based on the sensitivity of the data. Widespread use of the cloud may also encourage open standards for cloud computing that will establish baseline data security features common across different services and providers. Technical standards may develop over time (some noted that they are currently "all over the place" when it comes to the cloud), and innovation and flexibility may result from cloud computing. Cloud computing may allow for better auditing and data reliability since information is not as easily lost (when compared to the physical world).

Most respondents and participants agreed on the privacy risks raised by cloud computing. These generally relate to jurisdiction and accessibility by third parties and the principles contained in Schedule 1 of PIPEDA, including safeguards, limitation on uses and retention, and access and correction. One risk difference noted between the consumer and enterprise model, which was covered in the section on consent in online tracking, profiling and targeting above, was that the agreements between the vendor and the consumer tend to be "take it or leave it," while businesses can negotiate the terms of service. This leaves business with the ability to build in certain privacy protections, but consumers are often left less able to ensure their own protection.

III.III PIPEDA – Privacy principles

WHAT WE HEARD

PIPEDA – the regulatory framework

While most participants agreed on the challenges to privacy and data protection posed by the cloud model, there was some division as to whether PIPEDA was an adequate regulatory framework. Most were of the view that PIPEDA provides a robust and flexible regulatory framework in which to consider the privacy issues that result from cloud computing. According to most respondents and participants, PIPEDA's strength is that it is technology neutral, noting the fact that the OPC has been able to apply PIPEDA to new technologies and new business practices. Some, however, offered specific suggestions to strengthen PIPEDA. There was also some general discussion during the panels around whether a complaint-driven model is adequate for providing protection to consumers who are largely unaware of cloud computing. It was noted that proposed legislative amendments to make data breach notification mandatory will help make privacy practices more transparent to users and data protection authorities, and that this might encourage complaints to the OPC and, ultimately, better practices.

Many respondents and participants noted that cloud computing is simply outsourcing and that the issues that arise from outsourcing are the same. Who has control of the data? Who is accountable? Are there appropriate protections in place? Who has access to the data? With whom is it being shared? How is it being used? Are there jurisdictions where the data should not go? The concerns surrounding transborder data flows—a decades-old topic of discussion with respect to privacy protection—are brought into sharp focus in the cloud computing context.

Jurisdiction and third-party access

Cloud computing is largely borderless[50] as information in the cloud typically resides in different jurisdictions. It was noted by some respondents and participants that a business that utilizes the cloud model cannot outsource responsibility for protecting the data, noting that PIPEDA is quite clear on this in the section on accountability.[51]

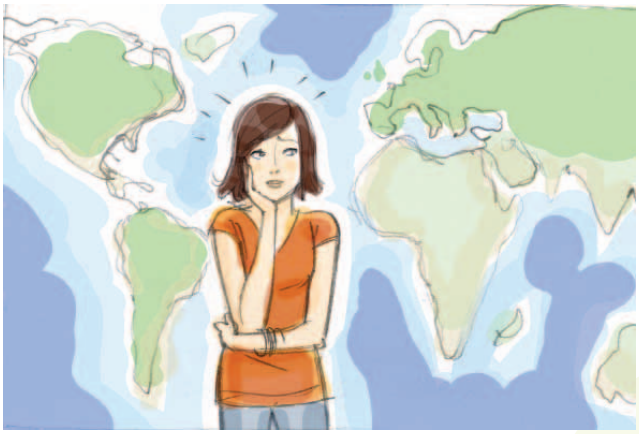
Canadian laws will continue to apply to the activities, but so too will laws in other jurisdictions.

A number of respondents remarked that greater transparency about the jurisdictions where data processing may occur is needed. It was also suggested that individuals should have the opportunity to opt out of certain processing if they do not agree with where the data are going.

Some suggested that a made-in-Canada solution is needed. Cloud computing that takes place solely in Canada may alleviate some of the concerns that are raised by data residing in or transiting other jurisdictions. However, one of the responses to the draft report did not support a "made-in-Canada" solution; noting the small size of the Canadian market, the organization asserted that a made-in-Canada cloud could not be ensured.

Closely linked to issues of jurisdiction are those related to access to the data by foreign governments. Comments were made that government access to personal information may be more complex in the cloud model than in other IT outsourcing arrangements.

Concerns were expressed about the risks of outsourcing personal data for processing in countries with laws that allow arguably easier access to the data on the part of governments than do the laws in Canada. Some were of the view that the risk of accessibility is not greater abroad than at home. Canadian laws provide for certain powers



that are analogous to those in other jurisdictions. Moreover, Canada has many formal and informal information-sharing agreements and arrangements with other jurisdictions.

The suggestion was made that there may be two options to reform PIPEDA in order to address the challenge of vulnerability of Canadians' personal information being accessible to foreign governments: creating a blocking statute and/or a proactive provision in PIPEDA to increase its deterrent value against disclosure. The blocking statute would prevent a domestic entity from complying with a specific foreign law, while the proactive provision would restrict extra-jurisdictional data processing.

The question of applicable law can be challenging for organizations. One organization noted that legal obligations can be conflicting at times, and that any geographic restrictions on data flows can make it more complicated. Such restrictions can curtail the development and benefits of cloud computing, and impose costs on users and service providers. Rather, it was suggested that any restrictions on data flows be preceded by a case-by-case assessment of the privacy risks that takes into account the volume and sensitivity of the information; the use and protection offered by technological safeguards; the likelihood of a foreign government actually asking for the information; the ability to target the information; and the probability and gravity of harm if the information were to be disclosed. The suggestion was made that governments should consider seeking a multilateral framework on cross-border data issues in the form of a treaty or similar international instrument. A less formal option was proposed in which countries could engage independently on procedures for resolving data access issues in ways that would avoid conflict around claims of jurisdiction.

In its response to the draft report, an advocacy organization expressed concern about the role of intermediaries with respect to certain public policy objectives. The organization is of the view that the cloud environment expands this situation, in which increasing amounts of information are entrusted to third parties and subject to disclosure upon request by a civil plaintiff or a government agent. The organization presented concerns related to proposed amendments contained in Bill C-29[52] and how these are exacerbated by the cloud model.

OPC observations

The OPC has considered extra-jurisdictional issues and accessibility by third parties in certain past complaint investigations. For example, we have examined the use of third-party processors in other countries and the obligations that were imposed on the organization that outsourced the data; we have also looked at a third-party processor that operated in multiple jurisdictions, including Canada, as well as the Canadian-based organizations that relied on it to carry out various business processes. We have been able to apply PIPEDA in all of these circumstances.

As a result of this work and in response to some concerns about how PIPEDA applied to transborder data flows, in 2009 the OPC issued *Guidelines for Processing Personal Data Across Borders*, which explains how PIPEDA applies to transfers of personal information to a third party, including a third party operating outside of Canada, for processing. These guidelines outline the approach contemplated under PIPEDA for protecting personal information that is being outsourced, organizations' obligations, and advice on how organizations can mitigate the potential risks from processing data across borders.

We are of the view that individuals have certain expectations of organizations, one of which is transparency in terms of the fact that their personal information flows across borders.

However, as noted in the Guidelines, the OPC recognizes the complexity of the electronic world and understands that it is often impossible for an organization to know precisely where information is flowing while in transit. That being said, the law is clear on where accountability lies, and organizations must, in their own best interests as well as those of their customers, do what they can to protect the information. We agree with many of the participants who noted that an organization cannot, through a contract, override the laws of a foreign jurisdiction.

While we recognize the concerns that underlie the suggestion that PIPEDA be reformed to prevent transfers of data to certain jurisdictions, we do not think that this is the answer. As a member country of the Organisation for Economic Co-operation and Development (OECD),

Canada agreed to the OECD *Guidelines for Governing the Protection of Privacy and Transborder Flows of Personal Data*, which represents the first internationally agreed-upon set of privacy principles and which is intended to support the goal of protecting the privacy of the individual while preventing any undue obstacles, in the name of privacy protection, to the free flow of data. PIPEDA is largely modeled on the principles outlined in the OECD Guidelines, and is intended to balance an individual's right to privacy with the need of an organization to collect, use or disclose that information for an appropriate purpose. We have long stated that we believe that privacy does not hinder innovation and economic progress. The organization-to-organization approach that underscores PIPEDA supports transborder flows and data protection by holding organizations to account for their personal information protection practices. Information is accessible to authorities regardless of where it resides. As noted in our Guidelines, we do, however, maintain our view that a careful risk assessment needs to be undertaken prior to any arrangement that involves the outsourcing of personal data to other organizations that operate globally, and that this assessment should consider the legal requirements of the jurisdiction in which the third-party processor operates, as well as some of the political, economic and social conditions, and any additional risk factors, in that jurisdiction.

Various treaties and agreements that may result in information sharing exist between Canada and other governments. With respect to information-sharing arrangements with other organizations, Treasury Board recently released *Guidance on Developing Information Sharing Agreements Involving Personal Information*.[53] The OPC was consulted on this document, and we provided input where we were of the view that privacy concerns needed addressing. We believe this document will help improve data governance.

When an individual such as Louise interacts with cloud applications or software, this is not outsourcing; rather, the company collecting the data from individuals is a data controller. PIPEDA has been applied to companies that were based in other countries and found to have had a real and substantial connection to Canada.[54] Ultimately, the OPC believes that a common approach to privacy across jurisdictions will help to ensure that privacy protections are in place and that businesses have common sets of rules to follow. To that end, the Office has worked hard with our provincial and territorial counterparts to provide consistent privacy approaches for citizens/consumers and businesses. Internationally, we continue to work with other data protection authorities towards mutual understanding and common approaches, as we believe businesses need to have consistency and citizens expect it. We have participated in and support the development of the Madrid Resolution[55]; we have also participated in the Accountability Project,[56] which has brought together a group of government, business and academic representatives to develop the concept of accountability. We participate in efforts by the International Organization for Standardization (ISO) to develop and maintain standards and guidelines addressing aspects of identity management, biometrics and the protection of personal information. ISO's key projects include developing framework standards for identity management and privacy, as well as identifying requirements for additional future standards and guidelines related to specific privacy-enhancing technologies.

In terms of enforcement, we have also recently been accepted as a participant in the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Enforcement Arrangement. The arrangement establishes a process under which participating authorities may contact each other for help with collecting evidence, sharing information on an organization or matter being investigated, enforcing actions, and transferring complaints to another jurisdiction. The OPC is also a member of the Global Privacy Enforcement Network (GPEN), which was formed in 2010 to share information about privacy enforcement issues, trends and experiences; participate in relevant training; cooperate on outreach activities; engage in dialogue with relevant private sector organizations on privacy enforcement and outreach issues; and facilitate effective cross-border privacy enforcement in specific matters by creating a contact list of privacy enforcement authorities interested in bilateral cooperation in cross-border investigations and enforcement matters. GPEN fulfills a 2007 OECD Recommendation that called on member countries to foster the establishment of an informal network of Privacy Enforcement Authorities.

Bill C-28, the "anti-spam" legislation (which received Royal Assent on December 15, 2010), amends PIPEDA to allow the OPC to share information with our provincial and international counterparts regarding personal information practices of organizations. We believe that this is a key change to dealing with privacy issues that arise from the globalization of personal information.

PROPOSED ACTIONS:

- The OPC encourages organizations to make it clear to individuals that their personal information may be processed in foreign jurisdictions and may be accessible to law enforcement and national security authorities in those jurisdictions. This must be done in clear, understandable language, ideally at the time the information is collected.
- The OPC will continue to provide guidance to organizations vis-à-vis transborder data flows.
- The OPC will continue to provide Parliament with our advice with respect to intergovernmental agreements and arrangements to share personal information.
- The OPC encourages Treasury Board Secretariat to continue to educate government departments that access data on commercial services regarding their privacy obligations, in support of its best practices for information-sharing agreements.
- The OPC respectfully urges Justice Canada to expedite its guidance document to government legal advisors concerning transborder data flows and third-party access issues.
- The OPC will continue to work towards harmonized approaches to data protection and enforcement.
- The OPC will co-operate where appropriate with our international counterparts to further the protection of personal information globally.

Safeguards

All respondents and participants noted that data security is one of the most important issues in cloud computing. While some may be of the view that the cloud poses certain security risks, others are of the view that it can strengthen security if the providers are able to use protection methods and technologies that would not normally be used by companies in their own individual data centres. It was noted that most cloud providers devote considerable resources to protecting information and authenticating users, and data security generally, with one organization noting that investments made by cloud service providers in security personnel and practices benefit all cloud users. The organization noted that technology has spread faster than people can be trained to manage it well. Another comment we received was that a cloud computing environment is more likely to be secure than most private IT environments.

One organization noted that cloud computing does not increase the risk of exposure and misuse of data (it is the same as with any third-party service provider), but rather increases the scale of an exposure. As pointed out, the aggregation of data can make a cloud data centre attractive to criminals.

Another organization commented that security is dependent on the cloud computing service provider's security controls and the customer's implementation of the cloud service. Data segregation and limiting access to data were considered important tools. Encryption was discussed, but one participant stressed that it is only one tool in a security strategy. One organization supports efforts to develop baseline privacy practices across the cloud industry that are largely modeled on the fair information practices in PIPEDA. It urged the OPC to keep in mind the work in other jurisdictions and such industry initiatives in any guidance that we develop to ensure consistency with approaches developed elsewhere.

There was general support for the development of very high standards of data security. One advocacy group was of the view that an independent or governmental body should be appointed to create and enforce standards; other participants, however, noted that the culture of technology innovation does not lend itself well to regulations and that, as a result, regulations lag behind technological advancements.

Mandatory breach notification was noted by many participants as being a useful means of shedding light on practices with the goal of improving privacy and security. It was noted that it is hard for individuals to complain about practices that they know nothing about. Many individuals do not even know that their personal information is in the cloud, and breaches often bring this out into the open. One very positive outcome of mandatory breach notification may be transparency. It was suggested by panelists that, with mandatory breach notification, regulators will have more awareness of what is going on and can offer guidance to improve practices. One panelist noted that perhaps a database of breaches should be kept to enable interested individuals to find out if their personal information has been compromised. It was also noted that to have a greater influence on practices, the Commissioner should perhaps have order-making powers.

We heard about different security challenges between the public and private clouds. With the public cloud, customers may have less control over security. It was noted, however, that the private cloud has its challenges, in spite of the "wall" that is created between the data and the rest of the Internet. People may not want others, even behind the wall, to have access to certain data, and access will need to be segregated to different people.

Mention was made about the different security risks between the consumer and enterprise models. Comments were made that more could be done with respect to data storage and data transfers in the consumer context, where security is often traded off in favour of usability and convenience. In contrast, security is a selling point in the enterprise model, with client expectations high. Enterprise cloud providers know this and make it a priority.

As detailed in the discussion on jurisdiction and accessibility, organizations that use a cloud provider are responsible for the data and need to specify certain requirements, including the location of the data, the ability of vendors to sub-contract, any limitations on access to the data, and audits. One participant noted that businesses can negotiate agreements with cloud providers while consumers tend to be presented with an all-or-nothing package. As one respondent argued, if consumers were as well aware as of the security risks as enterprise clients are, consumer cloud providers would have the incentive to be more stringent on security. However, consumers "do not have the luxury to educate themselves" as the respondent noted, arguing that technical safeguards in the consumer cloud market may be needed. Some noted that cloud services have been around for a while in the consumer space, and service providers have been applying a privacy framework to it.

One organization acknowledged that cloud providers do differ in their approaches to security and that these differences arise from various factors such as business and revenue models, consumer versus enterprise, or government customers. While it was of the view that different approaches to security are not a problem, what is problematic is that distinctions between providers' security practices are virtually invisible.

It was noted during the panel discussions that consumers need more and better information about issues related to the cloud in order to make an informed decision about a cloud provider, and organizations need guidance around what they can demand of the provider and what they should expect. For very small enterprises, such as Louise's jewellery business, the panelists had a variety of advice. One representative of a firm talked about how automated decision-making could be helpful to small entrepreneurs such as Louise. Others suggested that she do some research—not on the technology, but rather to find out what other similar businesses have used and what the benefits and risks were and how to mitigate them. She should ask trusted friends. It was suggested that the OPC could provide information to small and medium-sized enterprises on what issues to consider when using a cloud provider.

OPC observations

The OPC agrees that security of personal data in the cloud is paramount. How can Louise be sure, when she uses cloud services for personal reasons, that her personal information is protected? When Louise uses a cloud provider to help her with her business, how can she best find information to help her make the right decision? Can she be more demanding? How does she know what to look for or ask for? After all, Louise has obligations under PIPEDA to ensure that her customers' personal information is protected.

As noted in the online tracking, profiling and targeting section, building privacy in from the start—both in the technological and business process sense—is vital. It was stressed in the submissions and during panel discussions that the cloud can improve privacy and security, which is encouraging. We would agree with the comments we heard about the need for industry standards and strongly encourage development in this area. The proposed amendment to PIPEDA that would require mandatory breach reporting underscores the importance of personal information security and should help organizations that use technology and even those who develop it to better incorporate security into the technology. During the discussion, it was noted that when the OPC has reviewed how a breach occurred,[57] we look to industry standards to help us decide whether more should have been done—another important reason for such standards to be developed.

In addition to the need for standards, we agree with many of the respondents and panelists who are of the view that individual users and small and medium-sized enterprises need more information. We agree with the view that consumers need guidance concerning issues in the cloud, and organizations need guidance about what they need to do in the cloud.

It is also important to provide guidance to new service providers who are taking advantage of the rapid product development opportunities made possible by the cloud. "Apps" (applications) are becoming increasingly popular and sophisticated, but they do have privacy implications. An increasing number of application developers, aggregators and service providers are processing personal information that is either provided directly by consumers or passed on from host platforms. Some of these new players may not have the experience and motivation necessary to adequately protect individuals' privacy.

We noted the comment with respect to the Commissioner's powers. We are in the process of examining our own structure and function as a data protection authority. To that end, we commissioned a study[58] to look at the broad economic, legal and political context under which PIPEDA was first enacted, compared to the environment in which we find ourselves now. Part of this study is a comparison of our model against those of selected provinces and other countries.

Issues for feedback proposed in the draft report – Safeguards:

- We heard discussion about the need for standards and we urge organizations to develop strong personal information security standards. We would welcome further input on any work being done in this area in Canada, and any suggestions on what the next steps should be. The OPC is open to any comments industry would like to make in that regard.
- A suggestion was made that government undertake to develop such standards. We welcome further input on that suggestion.
- We heard about the security challenges in the public and private cloud models, but not the hybrid. We would welcome further input on the security issues that may arise from the hybrid model.

Response to issues for feedback

Of the five organizations that commented on cloud computing (one company, one industry association and two standards-related entities, as well as an advocacy organization commented on cloud computing but not specifically on standards-setting), there was general consensus that standards are needed. The company indicated that it favours industry-driven open standards. The association and two entities favour the established processes (which involve the private and public sectors, industry and academia) and argued that there is no need for government to undertake separate work to

establish standards. Input was provided on the standards development process; work is planned for developing cloud standards, but it has not yet started.

PROPOSED ACTIONS:

- The OPC will work with Industry Canada to consider how best to integrate privacy by design principles and PIAs into private sector practices.
- The OPC encourages the RCMP to conduct coordinated outreach to the private sector on data security and identity theft measures for consumers.
- The OPC urges organizations to develop standards that provide strong security protections. We will continue to track and contribute to work being done by ISO on cloud computing standards.
- The OPC will study further the management of personal information by application developers.
- The OPC will work on developing guidance for organizations on privacy considerations in the cloud.
- The OPC will also work on education initiatives aimed at individuals who use cloud services.

New uses, retention

We heard some discussion about function creep. Given the potential to profit from the large datasets they hold, some cloud providers may be tempted to use such information for other purposes. Behavioural advertising, also discussed in the consultations, is an example of how data could be used for other purposes; such a use would affect consumers such as Louise, who interact directly with consumer cloud services. The issue of using Louise's customer information was also discussed. Mention was made of transactional data (data that is created to describe a transaction) or datastreams, and how these could be used. One participant noted that there is a need for better "data hygiene." Given how inexpensive it is to keep data, there is little incentive to get rid of it and more incentive to do other things with it. In the enterprise model, the contracting organization (e.g., Louise, when acting as an entrepreneur) can put restrictions in place and ensure that consent is obtained prior to data being used in new ways. Two suggestions to address the problem were embedding in their systems restrictions on the kinds of uses that companies may make of collected data, and only collecting the data that are absolutely needed to provide the service; establishing data retention schedules will also be helpful in improving "data hygiene."

OPC observations

The OPC shares the concerns expressed by many about how data may be used. PIPEDA is quite clear that new collections, uses or disclosures require their own consent, and that collection of personal information must be limited to what is needed. Under PIPEDA, data can only be retained only as long as needed. Given the accountability model outlined in the Act, organizations that are contracting with a cloud provider are expected to impose certain restrictions and conduct audits. The greater concern appears to be in the consumer model, where the individual seems to have less control and where transparency and consent may be at risk. It may also be problematic for very small businesses that do not have the ability to conduct the due diligence needed before signing up with a cloud provider. Our requests for additional input and our proposed actions are contained in earlier sections of the report.

Access to one's personal information

The question of how individuals can access their personal information tended to be framed in the submissions and on the panels as one of ownership and portability. Indeed, this is an issue for Louise to consider, as she has obligations to her customers to provide them with access to and correction of their own personal information. Who owns the data? Can it be moved? Some wondered what happens to her data if Louise, for example, wanted to terminate her contract with her data provider. Can she get it back and make sure that it will not be used in the future? How does she get the data back in a format that

is useful? The comment was made that there are no guarantees about wiping data or giving it back in a useful format. Noting that many cloud providers do not allow users to easily retrieve or remove all of their data from the cloud if they wish to switch providers or cancel services, one respondent was of the view that this increases the barriers to users leaving and allows potential abuses of market power and user information. This individual suggested that removing barriers could alleviate many potential privacy concerns.

OPC observations

Consent and the ability to access and correct one's personal information are fair information practices contained in PIPEDA that give individuals control over their personal information. The other practices in essence protect that information and support the individual's ability to exert control. One concern the OPC has is that access and correction are not being facilitated on the Internet—though we do recognize that this can be challenging. The technology and the business models—and the sheer number of players involved—are making it very difficult for individuals to find out what information organizations hold about them and to fix any factual errors. This is of concern to us and ties into managing one's online identity and reputation, as well as security of personal information. With more information, users will likely raise more concerns, but we are of the view that industry needs to address the access and correction issues online.

PROPOSED ACTION:

- The OPC encourages industry to find innovative ways to meet the access and correction provisions under PIPEDA and welcomes further discussions on this issue.

CONCLUSION

For Louise and David, technology is mainly a source of entertainment and a way to socialize. Louise in particular takes full advantage of the many opportunities afforded to her online, including running her own business. She has concerns, however, about her personal information and that of her young brother, as well as the information of her jewellery customers.

There are many implications for our privacy when we live our lives online. When we are browsing, shopping, updating our status on social networking sites, or playing games, we leave information behind. This is information about ourselves and sometimes about others that can be used by organizations to make assumptions about us. Some of these assumptions can be used for arguably benign reasons, while other uses can have serious consequences. The security of this information is also of importance—who has it and what are they doing with it?

The aim of the 2010 OPC consumer consultations was to learn more about certain industry practices, explore their privacy implications, and find out what privacy protections Canadians expect with respect to online tracking, profiling and targeting, and cloud computing. The consultations were also intended to promote debate about the impact of technological developments on privacy, and to inform the next review process for PIPEDA.

As technology evolves, it is important that the balance between the needs of business and the privacy rights of individuals is maintained and reinforced where needed. We asked whether the tools we have now will be enough to protect privacy in the future. There is no easy answer.

Our interactions with technology, particularly in the online world, are causing the lines between our public and private selves to blur. Our children are affected too; increasingly, they are being given a digital presence before they can even say the word "no." Personal information protection will need to become a key component of digital literacy if we wish to continue to value our privacy and that of others. Greater emphasis will need to be placed on building privacy into technology and business models and more focus will need to centre on the ways in which we can manage our identities online.

Many consultation participants held the view that PIPEDA is working well as it is; others were less sure and offered suggestions for strengthening the framework. Our view is that, while PIPEDA has been able to adapt to technologies and business models that did not exist when the law came into force, there are challenges and we have concerns.

The second mandated five-year review of PIPEDA is approaching. It is clear to us that there are challenges in terms of how the Act is being implemented online:

- How is personal information being defined?
- How can meaningful consent be obtained in a way that is reasonable and clear?
- How can individuals access and correct their personal information in an online environment where data can be stored indefinitely and replicated?

When it comes to cloud computing, developing standards that will safeguard personal information is an area that needs focused attention. If anything, this exercise has helped shed light on practices that are largely invisible to individuals. The issue of transparency in an environment where many activities are technically complex for many people to understand is a serious one. Indeed, many individuals have little or no understanding of how their personal information can be used. The issues raised in the consultations have given us much to consider as we begin preparing for the second PIPEDA review process.

In addition to overseeing compliance with the law, we have another important role to play. In keeping with our mission to protect and promote the privacy rights of Canadians, we are undertaking specific activities to better inform citizens about their privacy online. In this regard, we will update information on our website for parents and teachers, young people, and small and medium-sized businesses about online privacy issues such as social networking, cookies, behavioural advertising, games and cloud computing. As well, we are continuing with research into privacy approaches that address some of the issues raised, including how best to inform individuals about practices, ways of obtaining consent, and how to better manage identity. This work will help inform our policy positions as the digital era progresses.

Canadians need to feel confident that they can embrace new technology and support new businesses without forfeiting complete control over their personal information. The 2010 OPC consultations are the start of our contribution to the discussion on how best to protect privacy in the 21st century.

APPENDIX A

SUMMARY OF ISSUES

Online tracking, profiling and targeting

Public/private divide and reputations

- The OPC would welcome further discussions with stakeholders on online identity management.

- The OPC challenges industry to find ways and means to help data expire and welcomes further discussions on this issue. PIPEDA is very clear that personal information should only be kept as long as it is needed.

Children need special attention

- The OPC welcomes comments on what baseline standards regarding children's personal information should be and how they can be developed. We also welcome views on what kind of framework should be put in place.

Consent, meaningful consent and transparency

- The OPC will continue to work with industry to develop the best approach to ensure that individuals are providing meaningful consent to legitimate business practices. This may be an area in which technology can prove helpful in addressing this problem. In that regard, we would welcome comments on how best to achieve this.

- The OPC will continue to focus our outreach activities on individuals to help them better protect themselves online. This will include exploring how best to help individuals focus on privacy explanations that are provided to them. We welcome any comments on how best to achieve this.

Other uses and disclosures

- The OPC welcomes additional views and comments regarding current and future online tracking and profiling practices (other than behavioural advertising) in Canada.

Cloud computing

Safeguards

- We heard discussion about the need for standards and we urge organizations to develop strong personal information security standards. We would welcome further input on any work being done in this area in Canada and any suggestions on what the next steps should be. The OPC is open to any comments industry would like to make in that regard.

- A suggestion was made that government undertake to develop such standards. We welcome further input on that suggestion.

- We heard about the security challenges in the public and private cloud models, but not the hybrid model. We would welcome further input on the security issues that may arise from the hybrid model.

ENDNOTES

1 Under paragraph 26(2)(b) of PIPEDA, the Governor in Council can exempt an organization, a class of organizations, an activity or a class of activities from the application of PIPEDA with respect to the collection, use or disclosure of personal information that occurs within a province that has passed legislation deemed to be substantially similar to the PIPEDA. Alberta, British Columbia and Quebec have private sector privacy legislation that has been deemed to be substantially similar. Ontario's *Personal Health Protection Act*, with respect to health information custodians.

2 PIPEDA initially covered only federal works, undertakings or businesses, and the collection, use or disclosure of personal information across borders. Hence, initial complaints were against businesses that fell into these categories.

3 See *Leading by Example: Key Developments in the First Seven Years of the Personal Information Protection and Electronic Documents Act (PIPEDA)* (OPC, 2008) http://www.priv.gc.ca/information/pub/lbe_080523_e.cfm

4 We are also examining genetic privacy. Smart technology is another area of interest to our work.

5 Dataveillance is defined as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons"; Roger Clarke, "IT and Dataveillance," November 1987.

6 http://www.kidscreen.com/articles/news/20100616/ipsos.html The study seems to suggest that very young children are online and interacting with websites and a variety of other media-playing devices. http://www.nngroup.com/reports/kids/ This study suggests that children are more experienced in using computers and the Internet and are exposed at fairly early ages.

7 See http://www.ftc.gov/os/2010/12/101201privacyreport.pdf In addition, on December 16, 2010, the U.S. Department of Commerce released its Green Paper, called "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework." The paper makes five recommendations: adopt a comprehensive set of fair information practices in the commercial context; increase cooperation among international data protection authorities; promote an enforceable voluntary code of conduct; create a new Privacy Policy Office within the Department of Commerce; consider developing a national standard for breach notification. See http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf

8 As of January 27, 2011, the webcast of the Toronto event has been viewed 1009 times. On the day of the event, the total Tweets hashtagged #priv2010 was 231, and the total number of page views to our consultation pages on the OPC website was 639. For the Montreal event, as of August 31, 2010, the webcast has been viewed 504 times. On the day of the event, the total Tweets hashtagged with #priv2010 was 193, and page views to the OPC's consultation web pages was 256. For Calgary, the webcast has been viewed 614 times as of January 27, 2011. On the day of the event, there were 161 tweets and 212 page views.

9 Retail idea based on a March 2010 story from RFID Journal: http://www.rfidjournal.com/article/print/7333

10 Ibid.

11 From http://www.networkadvertising.org/networks/Web_Beacons_rev_11-1-04.pdf

12 Ibid.

13 See p. iii http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf

14 http://www.piac.ca/privacy/piac_comments_to_privacy_commissioner_of_canada_on_behavioural_targeting

15 http://www.priv.gc.ca/parl/2009/parl_bg_20091208_e.cfm

16 http://www.piac.ca/privacy/tracking_consumers_online_behavioural_targeted_advertising_and_a_do_not_track_list_in_canada/

17 http://www.the-cma.org/downloads/regulatory/SubmissionAdvertisingMar10.pdf and http://www.the-cma.org/PublicUploads/224933BehaviouralAdvertising_09.pdf

18 "Research related to privacy and the use of geospatial information," Executive Summary, November 2009, prepared for Natural Resources Canada; http://epe.lac-bac.gc.ca/100/200/301/pwgsc-tpsgc/por-ef/natural_resources/2009/091-08/summary.pdf ; report can be found at: http://epe.lac-bac.gc.ca/100/200/301/pwgsc-tpsgc/por-ef/natural_resources/2009/091-08/report.pdf

19 From J. Stoddart's introductory remarks in Montreal, May 19, 2010.

20 Toronto panel on Location-based/Geospatial Tracking, April 29, 2010.

21 Toronto panel on Advertising, April 29, 2010.

22 See http://www.danah.org/papers/WhyYouthHeart.pdf

23 See http://pewinternet.org/Reports/2010/Reputation-Management/Summary-of-Findings.aspx?r=1

24 See http://www.danah.org/papers/talks/2009/SupernovaLeWeb.html

25 The OPC's strategic priorities are: information technology, identity management, national security and genetic privacy.

26 See Kim Cameron's Identity Weblog at http://www.identityblog.com

27 The OPC is funding a series of focus groups with parents, teachers, children and youth, in four regions across Canada, as part of the third phase of Young Canadians in a Wired World, a comprehensive and wide-ranging study by MNet of children's Internet use in Canada.

28 At the time of the production of this report, the amendment in question was included in Bill C-29, An Act to amend the *Personal Information Protection and Electronic Documents Act*, section 6.1.

29 See PIPEDA Case Summary #2003 – 162, http://www.priv.gc.ca/cf-dc/2003/cf-dc_030416_7_e.cfm

30 http://www.priv.gc.ca/cf-dc/2005/319_20051103_e.cfm and http://www.priv.gc.ca/cf-dc/2009/2009_010_rep_0813_e.cfm

31 http://www.priv.gc.ca/cf-dc/2006/351_20061109_e.cfm

32 http://www.priv.gc.ca/information/pub/rfid_e.pdf

33 See pp 20–25, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, February 2009. http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf

34 See http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

35 See http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp171_en.pdf

36 See http://www.futureofprivacy.org/2010/01/

37 Section 7 of PIPEDA lists the collections, uses or disclosures that may be made without knowledge or consent. See http://laws-lois.justice.gc.ca/eng/P-8.6/index.html

38 See http://www.priv.gc.ca/fs-fi/02_05_d_24_e.cfm for additional information.

39 See http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm. Note that the social ads feature has since changed on the site.

40 See http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

41 Subsection 5(3).

42 "How Companies are using your Social Media Data," *Mashable*, March 2, 2010 http://mashable.com/2010/03/02/data-mining-social-media/

43 http://www.fastcompany.com/blog/lucas-conley/advertising-branding-and-marketing/company-we-keep

44 For a discussion about the many players in the online advertising ecosystem, see http://news.ghostery.com/post/948639073/the-many-data-hats-a-company-can-wear

45 NIST cloud definition, version 15 http://csrc.nist.gov/groups/SNS/cloud-computing/

46 http://csrc.nist.gov/groups/SNS/cloud-computing/

47 Ibid.

48 Ibid.

49 "Data controller," "data processor" and "data subject" are terms found in the European Union's Data Protection Directive 95/46/EC.

50 Some cloud providers operate solely within Canada.

51 Principle 4.1.3 states that "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." See http://laws-lois.justice.gc.ca/eng/P-8.6/index.html

52 Bill C-29, An Act to amend the *Personal Information Protection and Electronic Documents Act*. The proposed amendments that the respondent is referring to are likely the lawful authority provisions.

53 See http://www.tbs-sct.gc.ca/atip-aiprp/isa-eer/isa-eer01-eng.asp

54 See http://www.priv.gc.ca/cf-dc/2009/2009_009_rep_0731_e.cfm and http://www.priv.gc.ca/cf-dc/2008/389_rep_080529_e.cfm for two recent examples.

55 See Resolution on International Standards of Privacy, 31st International Conference of Data Protection and Privacy Commissioners, 2009, http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf

56 See "Data Protection Accountability: The Essential Elements A Document for Discussion," Centre for Information Policy Leadership as Secretariat to the Galway Project, October 2009 http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf

57 For information on what the OPC does in response to privacy breaches, please see http://www.priv.gc.ca/resource/pb-avp/pb-avp_intro_e.cfm

58 See http://www.priv.gc.ca/information/pub/pipeda_h_s_e.cfm

NOTES

Office of the
Privacy Commissioner
of Canada

For more information

For general inquiries please visit our website at **www.priv.gc.ca** or call us

Toll-free: 1-800-282-1376
Tel: 613-947-1698
TTY/TDD: 613-992-9190
Fax: 613-947-6850

Follow us on Twitter: @PrivacyPrivee

Cat. No.: IP54-37/2011E-PDF
ISBN: 978-1-100-18396-1