Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Privacy, Trust and Innovation – Building Canada's Digital Advantage

Submission from the Office of the Privacy Commissioner of Canada
to the Digital Economy Consultation

July 9, 2010

Privacy, Trust and Innovation – Building Canada's Digital Advantage

Submission from the Office of the Privacy Commissioner of Canada to the Digital Economy Consultation

The Office of the Privacy Commissioner of Canada (OPC) is pleased to provide our submission in response to the Government of Canada's Consultation Paper on a Digital Economy Strategy for Canada, *Improving Canada's Digital Advantage: Strategies for Sustainable Prosperity*. We would like to thank the Government of Canada for providing the opportunity to contribute to this significant initiative.

We noted the many references to privacy in the consultation paper. The rapid pace with which technology has developed and continues to develop has implications for privacy. Privacy is key to the success of the digital economy, and can be a great motivator for innovation. 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. We have recently completed consultations on the privacy implications of online tracking, profiling and targeting, and cloud computing. We will be releasing a paper on these issues and what the privacy challenges may be in the near future. We welcome the opportunity you have provided to continue the dialogue and to offer suggestions on how Canada can be a digital and privacy leader.

Objectives of our submission

The OPC makes these submissions pursuant to its legislative mandate to protect the privacy rights of individuals and to promote the privacy protections available to Canadians. In our submissions, we will provide an overview of the work we have done with respect to digital technology and privacy, our perspective on the areas where privacy appears to be challenged by technological developments and business models, and how we think some of these challenges can be addressed in order to protect Canadians in the online marketplace in the years to come.

I Mandate and Mission of the Office of the Privacy Commissioner of Canada

The mandate of the OPC is to oversee compliance with the *Privacy Act*, which applies to the personal information handling practices of the 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 commercial activity (unless substantially similar provincial legislation is in place). PIPEDA also covers the personal information of customers and employees of federal works, undertakings and businesses.

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.

II OPC Focus

In recent years, the OPC has been involved in a number of activities that have highlighted how much has changed since Canada's privacy framework was put in place. Globalization, social changes, and the rapid pace of technological development have made the privacy environment a different place.

Through our investigations, audits, our research and policy work, our appearances or submissions regarding Bills, public opinion polling and environmental media scans, we are seeing very interesting technology and business models that pose fascinating challenges to how we have always viewed privacy protections.

For example, we made submissions to the Canadian Radio-television and Telecommunication Commission (CRTC) on the privacy implications of deep packet inspection, and we investigated its use as well as commissioned papers on it with a view to encouraging dialogue among Canadians. We have investigated social networking sites; we have met with various companies, at their request, over their proposed services that use technology in innovative ways, which have implications for privacy. We have focused on youth privacy by reaching out to young Canadians in an effort to help create good digital citizens. We continue to work with government departments through the privacy impact assessment review process to encourage them to find ways to build privacy into their programs and use of technology. But we know that what we have learned is the tip of the iceberg.

The timing of this consultation on a digital strategy for Canada is very timely. In the spring of 2010, we launched a consultation process into various online practices and technologies, namely online tracking, profiling and targeting of consumers by businesses, and the growing trend towards cloud computing, as a means for us to better understand the environment and the implications for privacy protection in advance of the next mandated five-year review of PIPEDA, scheduled for 2011. The consultations are linked to two of our strategic priorities: information technology and identity management. In 2007 we identified strategic priorities which we believe represent some of the most significant challenges to the privacy of people across Canada. These priorities guide our policy, research, investigative and audit work.

We are also in the process of examining our own structure and function as a data protection authority. To that end, we have commissioned a study 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.

Given that our consultations have just concluded and that we intend to produce a paper resulting from it in a few months time, and the study on our regulatory model is forthcoming, our submission on Canada's digital strategy will focus on general privacy issues that arise from certain technologies. We will also respectfully propose some actions that could be taken within our current privacy framework that would better promote privacy protection and support the trust needed to build Canada's digital advantage.

III Technology and Privacy

Canada's privacy framework

Technology has brought about many great conveniences for individuals. It has engendered

better services – as organizations have harnessed the power of the Internet to reach out to people – whether governments to citizens or companies to consumers. Technology has helped us do our jobs better – can we remember a time when we relied solely on the typewriter? It has inspired creativity in workers, in individuals, in citizens. It has a role to play in protecting our environment. Canada's future economic growth depends on innovation and on having strong frameworks in place to support its citizens as well as industry. In terms of personal information protection, Canada has been a leader in providing a privacy framework that supports organizations and protects the privacy of individuals. As Canada considers how best to improve Canada's digital advantage, it is important to ensure that that equilibrium is maintained, and reinforced where needed to ensure that Canada remains a privacy leader in the digital marketplace.

The development of a privacy framework in Canada (and indeed much of the Western world) has its roots in the evolution of technology and concerns over its potential effects on privacy. Starting around 40 years ago, as computers and databases became increasingly powerful, academics, policy makers and governments began to consider how best to protect the privacy of individuals.

In Canada, an extensive privacy framework was developed, beginning with the passage in 1978 of the *Canadian Human Rights Act* to cover the use of personal information by the federal public sector, followed by the passage in 1983 of the federal *Privacy Act*, and similar provincial and territorial legislation. PIPEDA, which regulates privacy practices in the private sector (unless substantially similar provincial privacy legislation is in place), was passed in 2000. PIPEDA incorporates the Canadian Standards Association Model Code, which was a model for self-regulation. The Code was based on the 1980 OECD *Guidelines for Governing the Protection of Privacy and Transborder Flows of Personal Data*, a document that represents the first internationally agreed upon set of privacy principles and which is intended to support both the goal of protecting the privacy of the individual (at least in terms of informational privacy) while preventing any undue obstacles, in the name of privacy protection, to the free flow of data.

The privacy principles laid out in PIPEDA have largely served both of these objectives well[1]. PIPEDA is a technology-neutral law, which so far has proven to be one of its strengths. The purpose of the law is to establish rules around personal information practices that recognize the individual's right to privacy with respect to personal information and the need of an organization to collect, use or disclose that information for an appropriate purpose. This focus on balance is important. In the nearly 10 years since it came into force, we have been able to apply PIPEDA to technologies and business models that did not exist when it was initially written. We have investigated social networking sites, and have dealt with interesting questions arising from street-level imaging technology used for mapping our cities. Our investigation, research and policy work continues to reach into other areas of the digital world.

Global digital economy

The globalization of personal information, the changes in how individuals interact with and

[1] The core fair information practices, as detailed in Schedule 1 of PIPEDA are as follows: accountability, identifying purposes, consent, limiting collection, limiting use, disclosure and retention, accuracy, safeguards, openness, and individual access

participate in technology, and the increasing pace of technological development have given policy makers, data protection authorities and observers in many countries pause. Are the principles we have hung our hats on for the last few decades going to serve citizens well in the face of evolving technologies? The OECD is preparing for a review in 2011 of its Guidelines; the European Commission launched consultations in 2009 regarding the European Directive[2]; the United States is pondering the merits of comprehensive privacy protection legislation; and work is afoot among many data protection authorities to find common ground on international privacy standards[3]. There is generally a recognition that not only has technology changed but that when it comes to personal information, the borders are disappearing and the landscape and players are evolving. Whether this means that the legislative frameworks we currently have in place will be up to the challenge is something that needs serious consideration.

The international component of this is significant with respect to this initiative because when we speak of "Canada's digital economy", we need to understand how technology is largely erasing borders. We are really speaking of a global digital economy, with more economies involved than only those in the Western hemisphere, some of whom may not have data protection laws. This has considerable implications for privacy and for business. Citizens want to know that privacy protections are in place, and businesses want to have a common set of rules to follow. For us, it can be very challenging to regulate the personal information practices of businesses that operate in multiple jurisdictions, where data regimes vary (if they exist at all).

At home, we have worked hard with our provincial and territorial counterparts to provide consistent privacy approaches for citizens/consumers and business. Internationally, the OPC continues 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 would like to stress that privacy protection is not an impediment to innovation and growth. Rather, privacy supports it by reinforcing confidence in individuals that the technology they use or that is used by the businesses they interact with is protecting their personal information by not only properly securing it from threats but also by supporting their rights to control their personal information. With confidence comes the support needed for innovation and economic growth in the digital economy.

The development of privacy-related standards for the use and deployment of new and existing technologies has been the subject of considerable debate and discussion within both the international standards community and the international data protection community.

The International Organization for Standardization, or ISO, signalled its intention to push ahead with this work with the creation of a working group on identity management and privacy technologies in 2006.

---

[2] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[3] Madrid Resolution, *Draft Joint International Standards on the Protection of Personal Data and Privacy*

Our Office has been an active participant in efforts by ISO to develop and maintain standards and guidelines addressing security 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.

It is not only privacy regulators who value fair information principles. In addition to the people who contact our Office with their privacy concerns, the importance of these principles has been brought to the fore in recent months by individuals in other venues, in very public ways. During the winter and spring of 2010, there was a plethora of articles appearing in news outlets and technical magazines in Canada and abroad that reflected the very real concerns that users have over issues of trust and control over their own personal information. We are referring primarily to the fallout from changes to the privacy settings used by one social networking site, and the implementation by another company of a new social networking application built on the use of its e-mail service. Both of the companies involved in these incidents are at the centre of the internet economy and are powerful innovators. However, their users showed great displeasure at what they perceived to be a fundamental change in the relationship that they believed they had with those companies. These incidents also highlighted how privacy considerations can be neglected during the design and testing phase of new technologies or the services built around them. This is an issue that we will return to later in this submission.

IV Privacy in the Digital Economy

Although the OPC consultations have just been completed and our policy position on these technologies has not yet been fully explored, it is clear that certain aspects of digital technology and the business models that use it or have evolved as a result of the technology raise certain privacy issues. If technology has blurred national borders, it is also blurring the distinctions between organizations, processors, and individuals.

Security of personal information

One of the key privacy issues that arise from technology concerns the security of personal information, as noted in the Government of Canada's consultation paper. Cyber security is a serious and growing concern. Security problems, particularly cyber crime and cyber espionage, are threatening our private and public e-infrastructures. There are a number of factors contributing to this problem:

- more electronic data being stored and processed
- ever increasing complexity of computer hardware and software
- ubiquitous computing devices that are often portable (smart phones, PDAs, laptops)
- a failure to use reliable software development methods that ensure security
- cyber criminals skilled at exploiting any discovered vulnerabilities
- the infection of millions of computers with bad software ("malware" or "crimeware")
- a developing e-crime economy that has perfected methods to convert stolen data into money

Cyber security is a complex problem that is proving to be very difficult to address although some computer companies are getting better at protecting their systems and software. In the meantime, cyber criminals have moved on to easier targets.

The scope of privacy protections and individual control

While security is an important issue, there are others that also have serious implications for consumers. We are on the cusp of a convergence of technologies that will provide comprehensive surveillance or "dataveillance" of individuals. From people writing about themselves and others on social networking sites, to mapping capabilities that show us and others where and how we live, to 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 one organization, to protect privacy or to invade it, that poses a significant challenge to protecting the online marketplace.

These developments raise questions about what personal information actually is. They raise questions about who is responsible for data protection when data is scattered in the clouds or when individuals disclose a great deal of personal data – their own and others' – on social networking sites. Digital technology highlights the challenges of ensuring that individuals have control over their personal information – can individuals understand the ways in which their personal information is handled, do they have the ability to meaningfully consent to various uses, and do they have access to their personal information? How long should data that has been amassed be kept? Storage is cheap and there are extenuating pressures to maintain data for longer and longer periods. What is the best way to protect the data? The scope of privacy protection, knowledge and consent, access, retention – these are the cornerstones of Canada's private sector privacy framework and ones that creators and users of digital technology need to understand and find ways to incorporate into products and services.

The following is not an exhaustive analysis of some of the current changing business models and technological advances and their privacy implications. Some of the privacy issues that arose from these developments could have been avoided or mitigated had the fundamental privacy principles been part of the planning and implementation processes. Some of these topics are currently the subject of our consultations. Others have been the subject of investigations or have implicated our Office's policy involvement as they have developed:

Social networking sites

Wildly popular and increasingly an integral part of our social and working lives, social networking poses interesting questions about where one draws the line between personal and commercial uses of personal information. It also poses challenges around questions of jurisdiction as many social networking sites are not Canadian-owned and operated. Such sites rely on personal information as a source of revenue to support a free service, which underscores concerns in some

quarters about the appropriateness of turning personal information provided willingly by individuals to communicate with family and friends into a currency. The degree of openness recommended to users when they post their personal information on the site, the amount of information given to users about how the site operates, and the practice of opening up the site's platform to developers to create applications for users and how much personal information is shared with developers are issues that have occupied our Office and merit continuing attention. Finding the balance between what the site needs to function as intended and how much control individuals want and can be technically given has been very challenging for both the companies and the Office.

Mapping technologies

The OPC worked with our provincial counterparts to develop guidance for companies planning on using street-level imaging technology for mapping services. Some of the privacy issues at play concerned consent and retention. We first became involved in this issue about three years ago when we learned of mapping services being launched in other countries and wanted to make sure that Canadians received privacy protection in keeping with our legislative frameworks. It was clear to us at that time that this was an issue that the company had not really given full attention to prior to the photographing of cityscapes.

Location-based services

Incorporating location of an individual into marketing strategies has become the Holy Grail in the technology industry. Marketers, internet search engines – they want to know where individuals are because location says a great deal about individuals and their habits, their interests, their friends. The prevalence of mobile devices and the increasing popularity of location-based applications are making it increasingly easy to paint accurate pictures of the movement and preferences of individuals.

The internet of things

The Internet of Things (IoT) is just one example of what has also been referred to as a sensor network. Sensor networks are a system of distributed sensor nodes interacting with each other and, depending on applications, interacting with other infrastructure in order to acquire, process, transfer, and provide information extracted from the physical world.

The IoT is described as "anytime, anywhere, by anyone or anything" computing and communications - it represents the convergence of several technologies including Internet Protocol version 6 (IPv6), Radio-Frequency Identification (RFID), wireless sensor technologies, smart technologies and nanotechnology.

We are already starting to see some of the precursors to the IoT in the deployment, for instance, of RFID as part of supply chain management and the introduction of advanced metering infrastructures for utilities, or smart grids. Other potential sensor networks include automation and control of smart homes, intelligent transportation systems and environmental observation, forecasting and protection.

There are a number of potential benefits that will arise from these technologies (singly or in combination), including RFID biosensors to warn of potential food contamination, remote monitoring of physiological parameters (elderly patients at home) and monitoring of habitat and environmental pollution.

These technologies (again, singly or in combination) also raise a number of privacy concerns. As these sensor networks become widespread, every object, every movement and every interaction online, and in some instances in the physical world, become pieces of data to be endlessly communicated, stored, mined and analyzed on countless levels.

For example, what user will remember that their new car automatically "phones home" to the manufacturer with maintenance and usage data? The online monitoring of home electricity usage may be useful for the consumer, but do consumers pause to consider how the utility may use that information – such as in a time of drought or a heatwave? How will the data produced by appliances and tools integrated into the smart grid be collected and analyzed, and by whom? These examples reflect challenges around what consumers know about how their personal information is used and whether consent was obtained.

Analytics

As databases of personal information grow, algorithms becomes more powerful and sophisticated, and data storage becomes cheaper, profiles of individuals can be constructed; once the Internet of Things becomes reality, those profiles can be further refined. People's activities, preferences, tastes, socio-economic status, education, and location can be gleaned from their use of technology. Thanks to increasingly powerful analytic capabilities, definitions of personal data and anonymity are being rethought, putting pressure on the fundamental scope of privacy frameworks. This has implications for giving open access to government-held research data as information thought to be anonymous may be less so once combined with other databases.

e-Health

The OPC and our provincial and territorial counterparts have been active in addressing the privacy issues related to personal health records (PHRs) initiatives[4]. Whether PHRs are developed by the private or public sector, we have called on all developers to ensure that the applications meet the relevant laws and reflect privacy best practices.

Evolving business models

Most of the examples above are largely enabled by Web 2.0. Web 2.0 is characterized by a radical shift in the way information flows and who provides it. As the line between content provider and

[4] See the federal-provincial-territorial Commissioners' resolution on *The Promise of Personal Health Records*.

content consumer becomes increasingly blurred, issues of control and responsibility have come to the forefront. Many platforms are now enhanced by third-party applications that facilitate the provision and sharing of content. The relationship between platform providers and third-party developers has raised questions around accountability for data collection, use, and safeguards. We confronted this issue during our investigation of a social networking site.

The subject of one of our recent public consultation events, "cloud computing" refers to a growing trend to outsource data storage and processing to third-party providers connected over the Internet[5]. Cloud computing is popular because it can greatly reduce the cost and complexity of running a local data centre. In addition, cloud providers who have specialized in a particular area (e.g., email, data mining) can provide advanced services that a single company might not be able to afford or develop.

Cloud computing can increase privacy and security capabilities 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.

Cloud computing does raise some privacy and security concerns, however. Data must be protected as it travels over the Internet and when it is stored in remote locations. Also, since cloud providers often serve multiple customers simultaneously, data must be properly segregated and protected from accidental and deliberate breaches.

Cloud computing also raises concerns about policy and jurisdictional issues. Customers of cloud services must ensure that the provider respects their values and policies about how data is handled. This is a significant concern if the data is stored in a jurisdiction different from where the cloud customer normally operates (e.g., a Canadian customer teaming with a U.S.-based cloud provider).

V. Recommendations

In developing a forward-looking policy agenda, there are a number of privacy-related issues that the federal government, industry, and the research and development sector need to consider. The consultation paper asks for input on the role the federal government could play in supporting the digital economy, and singles out certain ways that it can improve or increase its support. These include ensuring that the proper legislative or policy frameworks are in place; being a model user of digital technologies; building digital skills; supporting small- and medium-sized businesses; and funding for research and development. We offer recommendations within each of those areas where we believe that personal information protection can be improved while at the same time supporting innovation that makes Canada both a digital and privacy leader.

[5] This is a generic definition. There are many definitions of the term "cloud computing".

Legislative and policy frameworks

With respect to the recent introduction of new legislation (Bill C-29, *An Act to Amend the Personal Information Protection and Electronic Documents Act*) that amends PIPEDA to allow our Office to share information with our provincial and international counterparts, we believe that this is a key change to dealing with privacy issues that arise from the globalization of personal information. The introduction of 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 and the use of it. A positive outcome of mandatory breach reporting in other countries is that it has served as a catalyst for increased focus on data protection on the part of companies that operate in multiple jurisdictions.

Given our consultations and the upcoming legislative review, we will refrain from offering specific comments regarding the adequacy of PIPEDA's framework at this time. The paper that we intend to publish resulting from the consultations will focus on the privacy risks resulting from new technologies and where more attention or changes to legislation may be needed to mitigate these risks. In the meantime, we would offer the following comments:

Recommendation: Taking a holistic view and building privacy in from the start

As indicated earlier, PIPEDA is technology-neutral, grounded in the fair information practices, and thus far has been able to meet the challenges posed by evolving technology and business models. However, we believe more could be done to prevent privacy problems or mitigate the effects on privacy protection posed by new technology by making the existing privacy framework an integral part of the development of the digital economy. If the privacy protections that Canadians expect are to be respected and confidence in technology sustained, this is a vital step. Too often privacy is left out of the design stage, and fixes, after the fact, can be expensive.

This is not a new idea. For many years, privacy regulators, notably my Ontario counterpart, Ann Cavoukian, have been touting the benefits of considering privacy at the design stage (also known as "privacy by design"). In his opinion on promoting trust in the information society by fostering data protection and privacy, the European Data Protection Supervisor also advocates for a similar approach, recommending that relevant directives be amended to require that privacy by design be incorporated into the design process[6]. With a growing number of voices advocating for this step, the Government of Canada should consider ways in which this can be encouraged. Such a move has the added bonus of encouraging innovation in privacy protection through technology.

But that is not all that needs to be done. Privacy needs to also become an integral part of the business 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

[6] See *Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy*, Peter Hustinx, March 18, 2010

greater emphasis on such analysis may prevent problems from arising. The Government of Canada should consider ways in which PIAs can play a greater role in the private sector in bringing privacy into the equation.

Building a privacy culture, from design to implementation, needs strategies and support. We propose that the Government of Canada, along with the Office of the Privacy Commissioner of Canada, as part of its mandated role to promote the privacy protections available to Canadians, focus on the following areas in encouraging these developments:

Government as a model user

Recommendation: Strengthening privacy protections within the federal government

We agree that the federal government can play a crucial role in the development of the technology sector by being a "model user" of digital technology. However, from a privacy perspective, this may pose some challenges. The *Privacy Act* is nearly 30 years old. We had called on the federal government to undertake a review of the legislation given the changing landscape. Although the government has declined to do so, and while we continue to seek reform of the law, we have developed administrative measures to implement the "quick fixes" that we had recommended to the government. However, these are stop gap measures.

Nevertheless, a privacy regime is in place and it needs to be appropriately followed. We have recommended that privacy management frameworks be put into place, and some government departments have done so. We view this as a positive step. For its part, Treasury Board Secretariat is revising the PIA process. This is an opportunity to ensure that privacy is taken into account for all government programs, which is not always the case currently. We would like to see the PIA process be strengthened by including the requirement for a PIA analysis to be done as part of preparing Memoranda to Cabinet for program approvals.

We would also recommend that the government use state-of-the art authentication and protection technologies, an area where they are currently behind. Innovation in this area does not demand large-scale investment in custom solutions. For example, in the United States, the federal government is exploring how existing open-source standards and products can be used to provide identity verification as part of their online services.

The Government of Canada is taking positive steps towards addressing cyber security issues with the passage of Bill S-4, An Act to Amend the *Criminal Code*, and with the introduction of a bill concerning spam and another proposing amendments to PIPEDA. The RCMP has also started the National Strategy on Identity Crime. All of this work is very welcome; however, more needs to be done to ensure the security of personal information.

Citizen trust is vital and the Government of Canada should ensure that it is a model of privacy protection, as well as a model digital user.

Digital tools and skills

Recommendation: Making privacy literacy an integral component of digital citizenship

We agree that Canada needs to build digital skills for tomorrow. To that end, we would encourage an approach that includes privacy literacy as part of the tools needed for digital citizenship. If, from a policy perspective, we want to stress that privacy be part of the design and implementation of any technology, then the designers and users (both business and individuals) need to understand privacy obligations and their importance. This starts with their skills.

Part of any strategy to build digital tools needs to focus on young people. One of the recommendations to come out of the Canada 3.0 digital media forum in May was the creation of a national digital literacy initiative, with emphasis on the development of a "digital learning repository"[7]. We increasingly view online reputation management and privacy awareness as part of a suite of digital literacy skills necessary for success in a digital economy.

A recent report from the U.S. Pew Internet and American Life Project (2010) shows that many Internet users – and particularly younger Internet users between 18 and 29 – are actively managing their online identities by limiting the amount of personal information about themselves available online, changing default privacy settings on social networking sites, and other methods. Research from the Media Awareness Network (2005) suggests that a majority (66%) of Canadian children are not only concerned about digital privacy but seek out information on how to protect their privacy online[8].

Our Office is mandated with the role of educating the public about privacy issues. Our own anecdotal evidence gathered through my Office's presentations for school children, teachers, and parents (current reach to date: 18,000+) indicates that there is great interest in and demand for educational tools and resources.

Youth should not be the only focus, however. Developers, business leaders, users of all ages need to have a solid grounding in privacy principles if we are to protect Canada's online marketplace. Given that individuals post vast amounts of personal information about themselves and others – an activity that is largely outside the scope of PIPEDA – educating them on good privacy habits is vital.

---

[7] http://www.canada30.ca/blogs/learningstream/3learningstreamrecommendations

[8] http://www.pewinternet.org/Reports/2010/Reputation-Management.aspx

http://www.media-awareness.ca/english/research/ycww/phaseII/key_findings.cfm

Supporting small- and medium-sized enterprises (SMEs)

Recommendation: Providing tools to help SMEs better understand privacy

The consultation paper stresses the need to focus on SMEs in the development and use of digital technologies. The OPC has been targeting the same audience through its public education and outreach programs on their privacy obligations. The privacy message is becoming increasingly important as digital technologies are developed or adopted by these groups. For example, as technology becomes more complex, are SMEs maintaining their systems and therefore appropriately protecting any personal information they may have? Is cloud computing an attractive option for them? If so, what are the risks? PIAs or privacy audits may be highly useful ways of working through business practices and identifying privacy risks but they may be perceived as an added expense. Both Industry Canada and the OPC should help SMEs through the development of tools and education programs.

Recommendation: Targeting SMEs that are technology innovators

Many of the most innovative actors on the digital scene, notably application developers, fall into the category of small and medium enterprises. The application model attracts software developers working on their own or in small 2-5 person teams. We need to ensure privacy is considered at the design stage of application development by individual designers and developers. Targeting this group by providing tools, guidance, and education is another way of reaching some of the most innovative forces online.

Funding research and development

Recommendation: Funding privacy positive research and development

We agree that the Government of Canada should help support Canada's role in the digital economy through funding and research. We would like to see federal funding for security and network technologies that incorporate privacy protections. We would like federal funding of other technologies to include privacy protection as a criterion for any support. This would encourage the building of privacy into the development stage. Given the OECD's upcoming review of its Guidelines and the European Union's consultation on the Directive, this may be an opportune moment to work more closely with our international partners on finding ways to encourage privacy positive research and development.

Recommendation: Funding research to support digital literacy programs

Also important is the need for current Canadian research to support and focus digital literacy programs. The most recent research, the Media Awareness Network study, on behaviours, attitudes, and opinions of Canadian children and youth online is over five years old. In order to develop effective digital literacy tools, we need to better understand: Who is really vulnerable? To what degree? And what tools would they find useful? New research would also provide a true baseline for program

evaluation down the road. We would recommend that the Government of Canada explore the possibility of providing financial support to update the research that would provide us with comparable data.

VI Conclusion

Privacy protections are key to building trust in the digital economy and to protecting the online marketplace. Canada has been a leader in privacy protection and we believe it will continue to be so. Technological developments have long posed challenges to the privacy of individuals. Our privacy legislation and frameworks have largely held up well, but they will need support in the coming years to continue to find the balance between the individual's right to privacy and the need to advance and support our economy.