Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic
University of Ottawa – Faculty of Law, Common Law Section
57 Louis Pasteur Street
Ottawa, ON., K1N 6N5
cippic@uottawa.ca
www.cippic.ca

Digital Agenda:

A plan for Canada's digital society

July 14, 2010

Report By:

David Fewer, Director
Tamir Israel, Staff Lawyer
Jennifer Barrigar, Google Policy Fellow
Alexis Bowie, Summer Intern
Rachel Gold, Summer Intern
Colleen Hannigan, Summer Intern
Kent Mewhort, Summer Intern
Byron Pascoe, Summer Intern
Anca Sattler, Summer Intern

Table of Contents

OVERVIEW

CIPPIC commends the government on its decision to embark on this consultation process and to bring Canada back into a leadership position in the global digital economy. It is important that Canada join other nations such as the UK, the US, Belgium and Estonia in attempting to formulate a coherent national strategy for our digital development. In particular, the government's objective – for Canada "to have a world-leading digital economy; to be a nation that creates, uses and supplies advanced digital technologies and content to improve productivity across all sectors" – is laudable.[1]

CIPPIC is additionally pleased that the consultation document recognizes the need to instil consumer confidence and security in the digital marketplace. We are encouraged and hope that the government's digital strategy, when it arrives, will be informed by "a broad view of a digital economy or society".[2]

CIPPIC notes that Canada had not too long ago been a global leader on digital economic and social issues, and it is our hope that with this forthcoming digital strategy it can regain this position. To that effect, our submission is catered to addressing the needs of all Canadian constituents and sectors.[3]

[1] Canada, "Improving Canada's Digital Advantage: Strategies for Sustainable Prosperity" (May 2010), online: Digital Economy Consultation <http://de-en.gc.ca/wp-content/uploads/2010/05/Consultation_Paper.pdf>.
[2] Standing Senate Committee on Transport and Communications, "Plan for a Digital Canada" (June 2010), at 9-11, online: Plan for a Digital Canada <http://www.planpouruncanadanumerique.com/index.php?option=com_content&view=article&id=4&Itemid=13&lang=en>.
[3] S. Anderson, "A Digital Strategy for Whom? Industry or Society?" *The Tyee* (7 July 2010), online: The Tyee <http://thetyee.ca/Mediacheck/2010/07/07/DigitalStrategyForWhom/>.

I. Minister for Consumer and Civil Liberties Protection

Theme:	*Capacity to Innovate Using Digital Technologies*
Discussion Questions:	• *What would a successful digital strategy look like for your sector?* • *Are there new legislative/policy changes needed to deal with emerging technologies?* • *How can Canada use its regulatory and policy regime to promote Canada as a favourable environment?*
Recommendations:	**1. Facilitate dedicated consideration of digital customer and civil liberties protection issues by creating a Minister of Customer and Civil Liberties Protection;**

The digital environment is rapidly becoming embedded in every aspect of our day to day lives. The benefits of this new level of interconnectedness for individuals are inestimable and range from enhanced democratic participation, to unprecedented availability of knowledge bases, to self-empowerment. The risks that this rapidly evolving infrastructure poses to that sector of Canada's economy that is comprised of its citizens are equally great. In particular, the level of control and surveillance – whether by private or public actors – over every aspect of daily life that technology will enable in coming days is potentially limitless. Given this increasing ubiquity of interconnectedness, a significant and growing proportion of customer protection and civil society issues are now digital issues. It is essential that customer and civil society protections keep pace with the rapid development of economic innovation.

If Canada is to be a global leader in the digital world, it must do so on all fronts. For this to occur, customer protection and other civil society concerns will have to be considered from the perspective of customers and Canadian citizens in addition to industry. This requires a ministry whose primary focus is to advocate those issues across all areas of federal competency.[4] CIPPIC calls on the government to appoint a Minister of Customer and Civil Liberties Protection.

The creation of such a ministry will ensure that Canada remains a leader and innovator in crafting the global digital economy and society – now and in the future as new technologies emerge.[5] Without dedicated attention to customer protection and civil society issues, Canada may take steps to encourage a productive domestic digital economy but will ultimately have global innovations aimed at addressing such civil society concerns imposed on it from without. The digital infrastructure in which future Canadian citizens will conduct their economic and other affairs will be a product of multilateral concerns. If Canada intends to regain its leadership role in shaping that infrastructure, it must demonstrate a commitment to doing so on all fronts. A

[4] It is an additional feature of the digital world that issues of economy and consumer protection increasingly cut across provincial and national borders. Efforts to address customer protection and civil liberties will, when digital, typically have this cross-border dimension as well. A federal ministry dedicated to such issues will create a forum for coordinating Provincial consumer protection efforts as well as for ensuring Canada has input into the development of such changes on the international front.

[5] Michael Geist, "Building Confidence: Security, Privacy and User Empowerment – A discussion paper prepared for the Canada Roundtable on the Future of the Internet Economy", *Industry Canada: The Digital Economy in Canada* (2 October 2007), at 1, online: Industry Canada <http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00413.html>.

> Canada has long been viewed as an important participant in global policymaking, frequently serving as a bridge between divergent views from North America, Europe, and Asia… Canada's domestic agenda has the potential to serve as a role model for other countries grappling with these issues.

dedicated ministry focused on civil liberties and consumer protection issues will ensure digital economy and society issues are considered from *all* perspectives – including those of Canadian citizens – and will allow Canada to lead in forming the developing digital world. It will ensure that the emerging digital environment will be favourable for *all* sectors, including that comprised of its citizens.

II. Identity Theft

Theme:	*Capacity to Innovate Using Digital Technologies*
Discussion Questions:	• *How can Canada use its regulatory and policy regime to promote Canada as a favourable environment?*
Recommendations:	**2. Devote greater resources to tracking and studying the nature of identity theft as well as to manpower and training of law enforcement in the combating of identity theft;** **3. Establish victim recovery mechanisms such as universally accepted methods of attesting to identity theft; a right to an official declaration of identity theft victimization such as a detailed "Identity Theft Report"; a statutory right to free, one stop fraud alerts;** **4. Create a centralized entity with the funding and the mandate to address the identity theft problem and to educate the public as to its harms;**

Identity theft is in many ways the crime of the information age. Its perpetrators make use at every turn of the ever-growing information stores available online and elsewhere. Its social and individual costs grow daily. It is estimated that there are over 1 million individual victims of identity theft annually in Canada, with victim losses exceeding $3 billion.[6] This will only grow worse as new types of personal data migrate online and are increasingly aggregated in connection to each other. If the government wishes to increase confidence in the digital economy, there is no greater harm it must address than identity theft.[7]

The government has taken some recent steps to attempt to deter and reduce the incidence of identity theft in Canada. Foremost amongst these is the passage of Bill S-4, which criminalized many of the preparatory steps to identity theft. On the books are essential bills targeting online Spam and phishing (current Bill C-28, the Fighting Internet and Wireless Spam Act)[8] as well as imposing data breach notification obligations onto organizations (current Bill C-29, the Safeguarding Canadian's Personal Information Act).[9] Both of these long delayed Acts are essential steps in combating identity theft.

[6] McMaster University, "Measuring Identity Fraud in Canada: 2006 Consumer Survey", Working Paper #21 Abstract (2007), online: <http://www.merc-mcmaster.ca/working-papers/measuring-identity-fraud-in-canada-2006>, [*McMaster*].
[7] CIPPIC, Identity Theft/Fraud: Recommendations for Law, Policy and Institutional Reform: A White Paper, ["CIPPIC White Paper"], DRAFT, March 2010, forthcoming, draft on file with CIPPIC, at 5.
[8] Having passed 1st reading, online: Parliament of Canada <http://www2.parl.gc.ca/HousePublications/Publication.aspx?Docid=4547728&file=4>.
[9] Having passed 1st reading, online: Parliament of Canada <http://www2.parl.gc.ca/HousePublications/Publication.aspx?Docid=4547739&file=4>.

However none of these attempts are sufficient. While now enacted Bill S-4 and Bill C-28 take essential steps towards reducing the incidence of identity theft and deterring such activities, it is in the nature of the offence that full or even comprehensive deterrence is not a reality. Identity thieves are often quite sophisticated and technologically savvy, and in spite of the new remedies available to them, police and other administrative bodies will often lack the resources and training to track down the majority of identity thieves.[10]

Given the likelihood that most identity thieves will go free, much of the confidence-instilling activity the government must accomplish is on the remedial side. Identity theft is unique in that its impact on victims is often devastating – it is estimated that Canadian victims collectively spend approximately $164 million and over eighteen million hours of their personal resources in a year merely attempting to reclaim their good name and credit worthiness.[11] Much more can be done to alleviate this situation.

To begin with, potential victims must be made aware of the potential harms they are facing whenever their personal information is accessed without authorization. In this respect, as noted in greater detail below, the breach notification requirements found in Bill C-29 do not go far enough. That bill is fatally deficient in that it lacks any penalty for non-compliance with its breach notification requirements. Organizations have little or no incentive to comply. In addition, as noted below, there is no data breach notification requirement in Canada's federal Privacy Act, yet Canadians are no less exposed to identity thieves when their personal information is released by a public body than a private one. Breach notification is an essential aspect in preventing identity theft, as it permits Canadians to take remedial measures, to cancel or reissue identification documents, to be more aware of pre-texting attempts, etc.

Second, other jurisdictions have developed several remedial mechanisms that can help victims of identity theft regain their good names. Canada is far behind in providing such solutions.

This section addresses these various issues in the following order:

- What is Identity Theft?
- The Need for More Resources
- The Need for Victim Identity Recovery Measures
- The Need for Additional Victim Relief Measures

Issues relating to the need for breach notification on the private and the public sector are addressed in separate sections below. The recommendations put forward here are based on CIPPIC's extensive institutional experience with identity theft, which includes the production of a seven part series of working papers canvassing the issue as well as a forthcoming white paper providing far more detailed recommendations for addressing the issue of identity theft in a systematic manner.[12]

---

[10] CIPPIC White Paper, *supra* note 7 at 15-17. See also Bob Sullivan, *Your Evil Twin: Behind the Identity Fraud Epidemic* (Hoboken, New Jersey: John Wiley & Sons, Inc., 2004) at 144, who notes the disproportionate number of investigative hours required per the resolution of each identity theft offence.

[11] *McMaster*, *supra* note 6.

[12] More information is available at: <www.cippic.ca/identity-theft-2>.

A. What is Identity Theft?

The term "identity theft" is commonly used to refer to a range of crimes involving the theft and fraudulent use of another person's personal information,[13] including but not limited to government-issued "foundation documents," such as passports, driver's licenses, and birth certificates.[14] We shall use the term "identity theft" here to refer to the commission of any or all of the multiple steps involved in the commission of identity-related crime: (1) the collection of identity information and/or the creation of a fictitious identity; (2) the intermediate step of "breeding" (forging) and/or trafficking in identity information; and finally (3) the fraudulent use of that same identity information. [15]

While the most common purpose of identity theft is financial gain—identity thieves use their victims' personal information either fraudulently to access funds in existing credit, debit and other accounts, or to open new accounts in the victim's name for anything from credit and utilities to bank loans and mortgages—identity thieves also use personal information fraudulently to obtain health care services, employment, and rental accommodation, or to travel under an assumed identity or evade arrest.[16]

B. Needed: Resources for Law Enforcement

We need to ensure that police have the necessary human resources, including sufficient expertise in the sophisticated technologies used by some identity thieves (research indicates that the proportion of identity-related crimes committed by highly-skilled organized crime is increasing), to investigate identity-related crimes. Our research suggests that difficulties in investigating and prosecuting identity thieves stem largely from insufficient law enforcement resources to pursue identity theft investigations, which are frequently long and complicated. This is the challenge of identity theft. Identity thieves are often highly sophisticated, and investigations of identity thefts take on average 100 police hours, with complex cases averaging 500 hours.[17] We therefore recommend that governments provide law enforcement agencies with increased resources and training and manpower to investigate identity theft and assist victims.[18]

Law enforcement officials working to investigate identity-related crimes are also at a sharp disadvantage because many, if not all, cases of identity theft occur across multiple jurisdictions and, increasingly, across international borders, making it difficult to investigate and prosecute identity-related crimes.

Finally, law enforcement attempts would benefit significantly from a greater understanding on the scope and nature of identity theft in Canada. There is a lack of statistics on and tracking of identity-related offences in Canada.[19] There is a need for significant resources dedicated to tracking the problem and its dimensions as it exists in Canada.

---

[13] CIPPIC White Paper, *supra* note 7; See also CIPPIC, "Identity Theft FAQ", last updated June 2, 2007, online: CIPPIC <http://www.cippic.ca/index.php?page=id-theft-general/>.
[14] See W. Parkes, et. al., "Policy Approaches to Identity Theft: CIPPIC Working Paper No. 6", CIPPIC (March 2007), at 4-5, online: CIPPIC <http://www.cippic.ca/documents/bulletins/Introduction.pdf>.
[15] CIPPIC White Paper, *supra* note 7 at 4.
[16] See *Ibid*. at 6-7.
[17] CIPPIC White Paper, *supra* note 7, at p. 15, citing Sullivan, *supra* note 10.
[18] CIPPIC White Paper, *supra* note 7 at p. 15.
[19] CIPPIC White Paper, *supra* note 7 at p. 9, based on CIPPIC interviews with law enforcement officers.

Section Recommendations:

- greater identity theft dedicated resource for law enforcement training and manpower;
- greater resources dedicated to tracking the nature and scope of the identity theft problem in Canada;

C. Also Needed: Victim Recovery Measures

Identity theft is a uniquely harmful crime; it is immensely difficult for victims of identity theft to rehabilitate their reputation, and fraud re-occurrence using the same stolen or compromised personal information is common – often years in the future. In addition, victims find it difficult to convince credit agencies that questionable credit activity is, in fact, the result of identity theft, putting victims at a sharp disadvantage in credit and mortgage applications, possibly for the rest of their lives. The occurrence of identity theft in Canada is also growing: in 2009, Phonebusters National Call Centre reported that losses suffered by an estimated 11,979 Canadian identity theft victims totalled $10.8 million, an increase of $1 million annually since 2008.[20]

In Canada, victims of identity theft currently have three different methods of attesting to their victimization available to them: the Identity Theft Statement;[21] a police report ; and a Fraud Alert,[22] attached to the victim's credit report by the Canadian credit bureaus. None of these documents, however, are universally accepted as proving that an individual has been the victim of identity theft. Other jurisdictions offer stronger protections in each case.

i. Identity Theft Statement

To begin with, not all organizations accept the Identity Theft Statement. Some force consumers to use their own form. This lack of full standardization places a high burden on consumers in a time where they are already struggling to recover their identities.

In the U.S., the FTC has led a multi-stakeholder and industry wide effort to develop a universal standardized "Identity Theft Complaint" form that is incorporated into police reporting mechanisms.[23] The universal acceptance of this form by organizations greatly eases the burdens on victims. In addition, it facilitates the process of acquiring a police report for victims.

ii. Police Report

Canadians have found it difficult to acquire police reports on instances of identity theft. One problem is jurisdictional, with victims finding it difficult to access reports from investigations

---

[20] See *Ibid.* at 7-8.

[21] The Identity Theft Statement is a form intended to assist consumers by standardizing the process by which a consumer must prove they have been the victim of identity theft across several organizations. Each organization once had its own set of documents in distinct formats – a process that was extremely onerous on victims who are typically forced to prove their innocence to multiple sources at once. To alleviate this difficulty, a number of organizations have accepted a standardized form so that the victim need only gather the necessary information once and in one format. See: Phonebusters, "Identity Theft Statement: Instructions", online: <http://www.phonebusters.com/images/idtheftstatement.pdf>. See also CIPPIC White Paper, *supra* note 7 at 34.

[22] Fraud Alerts are notices placed on an individual's credit file upon request. Such alerts serve to notify credit organizations to be cautious before granting future credit to the object of the account while the alert remains in place. Currently, all three Canadian credit bureaus offer free Fraud Alerts on a voluntary basis (See CIPPIC White Paper, *supra* note 7 at 35-36).

[23] *Ibid*. at 34. See also: Federal Trade Commission, "Fighting Back Against Identity Theft" online: Federal Trade Commission <http://www.ftc.gov/bcp/edu/microsites/idtheft/tools.html>, [*FTC IDTheft*].

centered in distant jurisdictions and are given no local law enforcement point of contact.[24] To exacerbate matters, police often refuse to provide reports, or sufficiently detailed reports, of ongoing investigations to the victim herself.[25] This reticence appears rooted in standard police practice with respect to investigations of other offences. It can to some extent be remedied through better police education with respect to the specific exigencies of identity theft. As matters stand, the lack of a readily available police report detailing that the legitimacy of an instance of identity theft is a barrier to victims proving their innocence and regaining their identity and credit worthiness.

In the U.S., this issue has been partially addressed through the creation of standardized and universally recognized Identity Theft Reports as well as an accompanying process for producing these. An Identity Theft Report incorporates the Identity Theft Statement provided by the victim to police with a special police report that includes significantly more details than the standard report one might receive for investigations of other offences.[26]

Some U.S. jurisdictions take the extra step of providing victims with a statutory right to a local police report in cases of identity theft.[27] This ensures that victims will be capable of collecting at least that level of verification of the legitimacy of their claim of fraud. It additionally provides identity theft victims with a local point of reference for any follow up fraud they may experience.

iii. Fraud Alert

A fraud alert is a remedial measure victims can take in order to attempt to prevent further identity theft after an initial incident has been discovered. Currently, all three major credit reporting bureaus in Canada provide fraud alerts free of charge.[28]

In contrast, U.S. federal statutes go further, not only mandating that credit bureaus provide a free fraud alert upon request, but also requiring coordination and reporting mechanisms among different credit reporting bureaus so the victim need only convince one – an aptly named 'one-call' fraud alert.[29]

We recommend that government work to streamline the identity theft recovery process. Canadian identity theft victims typically need to deal with multiple organizations in order to rehabilitate their identity, each of which requires extensive written documentation that frequently takes the form of unique, organization-specific paperwork. The ability to point to a police report or fraud alert will greatly assist Canadians in legitimizing their claims of victimization, which often fall on deaf or sceptical organizational ears.

Specifically, we recommend the government work with stakeholders to create and implement a universally accepted affidavit/complaint form. Canadian identity theft victims typically need to

[24] *Ibid*. at 16-17.
[25] *Ibid*. at 34.
[26] *FTC IDTheft, supra* note 23, "What is an Identity Report".
[27] See *Spar* California Penal Code, s. 530.6, online: Justia US Laws <http://law.justia.com/california/codes/pen/528-539.html>.
[28] The Ontario *Consumer Reporting Act*, R.S.O. 1990, c. C-33, s. 12.1 mandates such alerts in the Province of Ontario.
[29] CIPPIC White Paper, *supra* note 7 at 35-36. See also *U.S. Fair Credit Reporting Act*, 15 U.S.C. 1681, s. 621(f).

deal with multiple organizations in order to rehabilitate their identity, and where each requires extensive written documentation in the form of unique, organization-specific paperwork, the harms of identity theft are exacerbated.

The government should in parallel encourage or legislate victims' rights to "Identity Theft Reports" akin to those available in the U.S. As noted above, the affidavit/complaint form will in many cases form the basis of the Identity Theft Report. Alternatively, a more official declaration of victimization can be offered, such as the "Identity Theft Passport" the Attorney General of the State of Virginia is authorized to issue.[30]

Finally, the government should work with Provincial governments to coordinate the adoption of statutory Fraud Alert requirements as well as a one-stop reporting mechanism analogous to that adopted in the US Fair Credit Reporting Act.[31]

Section Recommendations:

- Establish universally accepted form for establishing identity theft has occurred;
- Establish 'Identity Theft Reports' or analogous official statements verifying identity theft and providing far greater details than traditional police reports;
- Establish statutory rights to fraud alerts;

D. Urgently Needed: Better Coordination on this National Issue

We also recommend the creation of a national identity crime victim assistance centre. Such a centre can assist with many of the tasks highlighted above. It can be given a mandate for measuring, reporting and studying of identity theft offences. It can be a central source for ensuring that victims gain access to the remedial and reporting mechanisms described above. It can provide a legitimate point of inquiry for organizations to confirm and track identity thefts reported to them by victims.

In addition, such a centre can act as a focal point for education measures aimed at informing the general public on how to take steps to avoid identity theft.[32] Though information on how to prevent identity theft and what to do if you are victimized is widely available in Canada, both on-line and in print, it is spread across a huge number of disparate organizations. Canadians, therefore, would be well served by a single national website housing comprehensive information and links to resources for identity theft victims, such as the U.K.'s www.identity-theft.org.uk or the U.S.'s recently-created www.idtheft.gov.[33] Canadian identity theft victims are usually unaware not only of the steps they need to take to rehabilitate their identities, but also of their legal rights. A national website should therefore also provide a quick-reference guide to identity theft victims' rights, as should the credit bureaus to whom victims are encouraged to report fraudulent activity occurring in their names.[34] Victims should also have access via a toll-free telephone number to advice, counselling, and assistance with the process of restoring their identity, such as is currently offered in the U.S. by the ID Theft Resource Centre. Thus we

---

[30] Commonwealth of Virginia, "FAQ: Identity Theft", online: Commonwealth of Virginia <http://www.oag.state.va.us/faqs/faq_idtheft.html>.
[31] See *supra* note 29 and accompanying text.
[32] See CIPPIC White Paper, *supra* note 7 at 33.
[33] See *Ibid*.; See also online: Identity Theft <http://www.identity-theft.org.uk/>, <http://www.iftheft.gov>.
[34] See CIPPIC White Paper, *supra* note 7 at 33.

recommend the establishment of a similar national identity crime victim assistance centre, with a mandate to provide the Canadian public with complete and up-to-date information on preventing and rectifying the harms caused by identity theft.

The Government can create an independent agency to focus primarily on identity theft or, alternatively, provide the Consumer Measures Committee or other similar institution such as the Privacy Commissioner of Canada with the mandate and the resources to carry out a concerted campaign against identity theft similar to that accomplished by the U.S. FTC.

Section Recommendations:

- Create a centralized entity with a mandate and budget to track and address identity theft issues;

Conclusion

As the digital economy continues to grow, both in size and in prominence in the lives of Canadians, so too does the risk to consumers of becoming identity theft victims. The government, therefore, must take an active role in advancing new, and vigorously enforcing existing, consumer protections.

III. Issues in Identity Management

Theme:	*Growing the Information and Communications Technology Industry*
Discussion Questions:	• *Do current investments in R&D **effectively** lead to innovation, products and services?* • *What is needed to innovate the ICT industry?*
Recommendations:	**5. Government should provide incentives in the form of grants for innovators to study and develop identity management systems that further public policy objectives such as online anonymity/free expression, privacy, and security.**

Individuals are engaging in a growing number of online transactions with a growing variety of online service providers. Increasingly, these online services are requiring users to provide more and more personal information in order to access their applications – much for secondary purposes not directly linked to the primary service being offered. In addition, more business and government services are migrating to the digital world, meaning there will be more and more personal and sensitive data online. This is particularly troublesome considering the number of security breaches that occur every year, exposing people's private information to the world at large, as well as the prevalence of identity fraud.[35] Aside from the increasing concentration and availability of personal information online, a contributing factor to this growing prevalence is general practices of the common internet user, who typically uses the same login/password combination across numerous accounts in order to simplify the memory burden of managing her online identity (the average user has around 25 password-protected accounts and types 8

[35] Privacy Rights Clearinghouse, *Chronology of Data Breaches*, (last updated July 13, 2010), online: Privacy Rights Clearinghouse <www.privacyrights.org/ar/ChronDataBreaches.htm>.

passwords a day).[36] This means that a data breach at one website could create a ripple effect across all sites that an individual visits.

Partially in response to this situation, a number of private organizations are offering and developing identity provider services which purport to help users create, manage and share their digital identities more securely and with greater ease. Instead of providing the same password to every website visited, Canadians can create one centralized ID and use that single account to sign in to thousands of websites.[37] In most services of this nature, the user's password is only shared with the identity provider and not with every website visited.[38] Furthermore, users can store personal information with the identity provider which can then be used to automatically fill out the required registration forms, as opposed to the user having to repeatedly provide that information to every site visited.[39] While this might be an efficient solution and may alleviate some of the mental burden users currently face, there remain serious vulnerabilities within these identity management systems that have the potential to put an individual's sensitive information at even greater risk.

A. Identity Management Systems

Despite the fact that there is significant value in protecting online anonymity, there are certain types of interactions, such as banking and online health services, that require the parties involved to have a high level of trust in each other's identity.[40] To create the kind of trusted environment that can facilitate these increasingly complex interactions, mechanisms have developed to attempt to authenticate an individual's digital identity.[41] As CDT notes: "[t]his process of claiming identity, authenticating identity, and authorizing that identity to use certain services is known as Identity Management."[42] By providing a stable means of identity authentication, identity management systems could potentially be helpful in reducing fraud and identity theft. However, to be successful they need to be designed in a way that prioritizes user privacy and data security in order to protect the personal and often highly sensitive information of users. One proposal to help achieve this is to ensure that individuals remain in control of their own information as much as possible.[43]

However identity management can also increase security risks and risks of fraud and identity theft. There are, in fact, potentially inherent contradictions in the identity management model which may counteract the secure and trust-enhancing ecosystem such utilities are intended to

---

[36] Rachna Dhamija & Lisa Dusseault, "The Seven Flaws of Identity Management", *IEEE Security & Privacy* (March/April 2008), at p. 25, online: Harvard School of Engineering <http://people.seas.harvard.edu/~rachna/papers/seven-flaws-of-identity-management.pdf>.
[37] OpenId, *Benefits of OpenId*, online: OpenID <http://openid.net/get-an-openid/individuals>.
[38] *Ibid*.
[39] *Ibid*.
[40] National Science and Technology Council Subcommittee on Biometrics and Identity Management, *Identity Management Task Force Report 2008*, at 1, online: Biometrics <http://www.biometrics.gov/Documents/IdMReport_22SEP08_Final.pdf>.
[41] *Ibid*.
[42] Center for Democracy & Technology, "Issues for Responsible User-Centric Identity" (November 2009), at 1, online: Center for Democracy & Technology <http://www.cdt.org/files/pdfs/Issues_for_Responsible_UCI.pdf>.
[43] Eve Maler & Drummond Reed, "The Venn of Identity: Options and Issues in Federated Identity Management" *IEEE Security & Privacy* (March/April 2008), at 19, online: Pushing String <http://www.xmlgrrl.com/publications/IEEESecPriv-MarApr2008-MalerReed-Venn.pdf>.

provide. Identity management systems developed to date typically introduce a third party identity provider that manages a user's personal information and conducts authentication tasks. While such services attempt to be user-centric, the extent to which this can be achieved is questionable. For example, it has been well documented that, when prompted, users often disclose too much and might simply agree to release information through easily dismissed and repetitive mechanisms if it is the most efficient way to reach their goal.[44] As ease of information exchange is the currency in which identity management systems exchange, such ease of transfer is only likely to exacerbate these unproductive user habits towards over disclosure.[45] This is particularly troubling when one considers that these identity providers are proposing to hold all of an individual's personal information, necessarily suited to multiple diverse services, within the provider's servers. Such localization of increasingly sensitive data sets poses an additional and significant threat to Canadians from data breach. As one commentator rightly noted: "[s]ince identity federation is likely to go along with the exchange of sensitive user information in a highly insecure online environment, security and privacy issues associated with such exchanges are key concerns."[46]

B. Security Risks

Despite the fact that there are security risks associated with using the same or similar identifiers for a variety of websites, "federated identity systems that let users leverage one credential across many sites will only increase the value of the credential as a phishing target."[47] While internet browsers such as Mozilla Firefox are making it easier for people to detect illegitimate phishing or pharming websites, it is still important for users to be able to authenticate not only their identity provider but relying parties as well.[48] However, as Dhamjia and Dusseault note, even where the relying party *can* be authenticated for the user's benefit, such authentication may lead to *false* user trust/confidence and even greater exposure:

> Unfortunately, there will be no guarantee that a relying party that behaves well today will continue to do so tomorrow; a site could build up trust and then abuse it.[49]

The question of who users can trust with their identity information involves an assessment of risk which can be very difficult for individuals, particularly when it involves decisions about their privacy and security.[50]

---

[44] Dhamija & Dusseault, *supra* note 36 at 26.

[45] Facebook describes the benefits of *its* authentication service as such:

> By using Facebook instead of a web form, a new user can provide all of the information required for site registration with a single dialog (no typing required!). Likewise, the information is more reliable than the information you would get in a web form. For example, the email address provided via Facebook has been verified by Facebook, so it does not need to be re-verified by your site.

Facebook Developers, "Facebook for Websites", online: Facebook <http://developers.facebook.com/docs/guides/web>.

[46] Gail-Joon Ahn & John Lam, "Managing Privacy Preferences for Federated Identity Management" 2005 ACM Workshop on Digital Identity Management, at 28, online: Radboud University Nijmegen <http://www.cs.ru.nl/~jhh/pub/secsem/Managing%20privacy%20preferences%20for%20federated%20identity%20management.pdf>.

[47] Dhamija & Dusseault, *supra* note 36 at 26.

[48] *Ibid.*

[49] *Ibid.* at 27.

[50] *Ibid.*

Data needs to be secured both in its transmission and in its storage. However, there are numerous examples of established and reputable organizations that have experienced security breaches and that have lost control of databases containing sensitive data: "[a]uthentication schemes, even those that security experts currently recommend and responsible organizations use, can be flawed, attacked, or poorly implemented."[51] When all of an individual's information, from health to banking to employment, is stored in one location, a security breach or change in relying party practices could have severe consequences.

C. Privacy Concerns

The idea of a user going through an identity provider for all of their online transactions presents a number of privacy concerns. There are critical questions that remain unanswered around the type of data that can be collected, how it can be used, how long it can be retained as well as if and how it needs to be destroyed.[52] Furthermore, if users are going to hand over this information to identity providers, fair information consent practices must be enforced diligently. It must be clarified that relying parties cannot demand personal information for secondary purposes such as marketing as a condition of service. Further, consent in such contexts must be express. The identity provider must require opt-in consent for all unnecessary data sets *as well as for all unnecessary purposes*. Additionally, users should have the option of revoking consent and having their data removed.

As previously mentioned, there are certain circumstances under which individuals should be allowed to interact online anonymously. Some degree of anonymity "has significant safety value and is in keeping with what should be perceived as being good public policy."[53] Such anonymity furthers both privacy and free expression – values enshrined in our *Charter*. In light of this, identity management systems should also incorporate better techniques to enable users to remain unidentifiable for certain purposes. Related to this, there needs to be limits imposed with respect to data aggregation, mining and profiling, as well as to the conditions under with such data can be lawfully disclosed to government agents. This raises significant issues because online behaviour can be tracked and linked to an individual user: "[t]he more data gathered the easier it will be to trace who did what."[54]

D. Government Involvement

The government has a role to play in encouraging the development of identity management solutions that are in line with broader public policy objectives such as online anonymity, privacy, and security. While "[m]arket forces encourage architectures of identity [in order] to facilitate online commerce",[55] the government's role should be "to ensure that those public values that are not in commerce's interest are also built into the architecture."[56] The government should

---

[51] *Ibid.*
[52] Center for Democracy & Technology, "Issues for Responsible User-Centric Identity", (November 2009), at 8, online: Center for Democracy & Technology <http://www.cdt.org/files/pdfs/Issues_for_Responsible_UCI.pdf>.
[53] *Warming v. Fournier,* [2010] ONSC 2126 (Ont. Div. Ct.) at para. 20, citing *Irwin Toy Ltd. v. Doe,* [2000] O.J. No. 3318 (S.C.J.). See also generally, I. Kerr, *et al*., "Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society", (NY: Oxford University Press, Inc., 2009), online: ID Trail <http://www.idtrail.org/content/view/799>.
[54] Lawrence Lessig, *Code 2.0* (NY: Basic Books, 2006), at 77, online: Codev2 <http://pdf.codev2.cc/Lessig-Codev2.pdf.>.
[55] *Ibid.*
[56] *Ibid.*

consider funding research into identity management systems to ensure that they are designed with privacy and security as central defining features. Such alternatives to the current business models will ensure that individuals are able to retain as much control over their sensitive personal information as possible, that this information is secure and that their privacy online is protected. The government should provide incentives for innovators to create models that aim "to give users total control over their identities, even letting them host their own identity providers (or letting them dictate where they're hosted), as well as control authentication and attribute exchange."[57] Empowering users represents a technical challenge, however, it could be one way to protect individuals.

As noted by Lawrence Lessig in his seminal work, Code:

> As the world is now, code writers are increasingly lawmakers. They determine what the defaults of the Internet will be; whether privacy will be protected; the degree to which anonymity will be allowed; the extent to which access will be guaranteed."[58]

It is important for the government to ensure, in light of this, that the innovators and code writers are provided with incentives that reflect important public policy objectives such as free expression, privacy and security. These are not values to which the market has historically catered to in an efficient manner. It is for this reason that we entrust to government the role of ensuring such public values are prioritized. This should no less apply to the design of something as important as future identity management systems.

IV. Intermediaries

Theme:	*Capacity to Innovate Using Digital Technologies*
Discussion Questions:	• *What would a successful digital strategy look like for your sector?* • *Are there new legislative/policy changes needed to deal with emerging technologies?* • *How can Canada use its regulatory and policy regime to promote Canada as a favourable environment?*
Recommendations:	**6. Examine the need and possibility of applying basic due process and proportionality obligations on intermediaries when carrying out roles of a public character;** **7. Inspect internal legislative agendas and co-regulatory activity to ensure that it does not facilitate disproportional impact on important Charter principles;**

A central feature of the digital world is that access to content, to social interactions, to various aspects of the marketplace, to just about everything is increasingly mediated through third parties – intermediaries.[59] Online intermediaries are many and varied.[60] They play essential roles by

[57] Maler & Reed, *supra* note 43 at 19.
[58] Lessig, *supra* note 54 at 79.
[59] This trend whereby aspects of our daily lives are mediated to increasing degrees will only grow with time as the Internet transitions from a network of interconnected computers to a network of interconnected mobile devices and, ultimately, to a network of interconnected objects: see A. Clement and K.L. Smith (conveners), "Consensus Submission to Digital Economy Strategy for Canada: A document prepared through a consensus-based roundtable process", *University of Toronto, Faculty of Information* (9 July 2010), at 24-25; EU Commission of the European Communities, "Commission Communication on the Internet of Things – An action plan for Europe", COM(2009

facilitating online interactions that could not be achieved without an intermediary. In so doing, they empower individual Canadians and individuals across the world to interact in new and beneficial ways. At the same time, however, this growing level of intermediation that the digital world facilitates is accompanied by potential for unprecedented levels of control and surveillance over all aspects of the lives of Canadians.[61] Intermediaries are increasingly exercising this potential, often at the behest of policy makers, to achieve what were once considered exclusively public policy objectives such as police surveillance,[62] adjudicating and enforcement of intellectual property rights,[63] fraud detection, adjudication and enforcement of defamatory speech,[64] to filtering of criminal content.[65] Moreover, the international trend appears to be moving towards greater reliance on such private entities to achieve an ever-increasing range of public policy objectives.[66]

---

278 final), online: European Commission <http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf>.

[60] The OECD describes internet intermediaries as private entities which:

> …bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties.

OECD, "The Economic and Social Role of Internet Intermediaries" (April 2010), at 9, online: OECD <http://www.oecd.org/dataoecd/49/4/44949023.pdf>.

[61] Lessig, *supra* note 54, generally. See also, I. Kerr, "The Strange Return of Gyges' Ring: An Introduction", in I. Kerr, *et al*., *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, (NY: Oxford University Press, 2009).

[62] See *Spar R. v. Cuttell*, [2009] O.J. No. 4053 (Ont. C.J.) at para. 79-80 [*Cuttell*].

[63] See M. Geist, *Cyber Law 2.0*, (2002) B.C. L. Rev. 323 at 338-339, describing how Canadian intermediaries, fearing copyright liability in foreign jurisdictions, take down content posted by Canadians without attempting to assess whether such content would be in violation of Canadian copyright laws. See, additionally, the Canadian Internet Registration Authority's dispute resolution process, which permits CIRA to identify otherwise anonymous domain name owners upon receiving a 'good faith' allegation of IP infringement (CIRA *Request for Disclosure of Registrant Information – Rules and Procedures Version 1.4*, at s. 3(b), online: Canadian Internet Registration Authority <http://www.cira.ca/en/document/disclosureregistrant.pdf>). Contrast this to the higher judicial standard the Ontario Divisional Court recently found was necessary to preserve online anonymity in light of good faith allegations of defamation (*Warman v. Fournier*, [2010] O.J. No. 1846, 2010 ONSC 2126 (Ont. Div. Ct.)). See also B. Sookman and D. Glover, "Graduated Response and Copyright: An Idea That is Right for the Times", , (20 January 2010), online: Barrysookman <http://www.barrysookman.com/2010/01/20/graduated-response-and-copyright-an-idea-that-is-right-for-the-times/>, for an extreme example.

[64] Canadian intermediaries such as website hosts appear to have an obligation to take down content *allegedly* defamatory if they are made aware of it: A.M. Linden and B. Feldthusen, *Canadian Tort Law*, 8th ed., (Markham, ON: LexisNexis Canada Inc., 2006) at 784, and particularly at note 195.

[65] All of Canada's major internet service providers as well as CAIP, a coalition of many of Canada's smaller Internet competitive resellers have on their own accord implemented Project Cleanfeed, which filters all online traffic for images and websites in violation of child pornography laws and blocks these: M. Geist, "Project Cleanfeed Canada", (24 November 2006), online: Michaelgeist <http://www.michaelgeist.ca/content/view/1548/125/>.

[66] Geist, *supra* note 63 at 351 *et. seq.* points to an increasing willingness to regulate internet intermediaries by government entities in order to achieve public policy objectives. See also J. Goldsmith, *et al.*, "Who Controls the Internet? And Army of Davids", *Slate*, (28 March 2006), online: Slate <http://www.slate.com/id/2138537/entry/2138574/>. The more recent trend appears to be shifting towards a range of regulation directly deputizing intermediaries to carry out public policy objectives mixed with a perhaps more insidious dose of co-regulation, where private intermediaries are pressured into taking on public policy objectives through indirect pressure or threat of regulation. In the latter case, it is not clear whether and to what extent the *Charter* applies to their actions.

Historically, private sector organizations have lacked the institutional capacity to properly conduct the types of public roles currently being thrust upon intermediaries, for a number of reasons. First, private organizations such as intermediaries, while capable of exerting a significant amount of power and control on individuals and on Canadian society at large, are not subject to democratic forces.[67] Nor are they subject to the same system of checks and balances that allows public bodies such as the executive, the legislature, and our network of judicial and quasi-judicial actors to properly balance the competing public policy objectives currently faced by many private intermediaries.[68] So, when setting standards with sweeping implications for significant subsections of Canadian society through terms of use contracts and internal policies, these intermediaries are not subject to the same incentive systems typically relied upon in a free and democratic society to ensure the proper balance is struck between competing social values.

Second, private actors such as intermediaries by and large lack the expertise and the resources necessary to properly implement public policy objectives. Such entities are perhaps the most efficient mechanism for maximizing innovation and productivity, but, again, not necessarily for achieving the nuanced decision-making typically necessary to properly adjudicate private rights disputes[69] or to effectively decide when *Charter* protections such as those found in s. 8 should or should not be bypassed.[70]

Finally, private intermediaries lack the moral legitimacy to carry out comprehensive public policy agendas in the manner that they are increasingly called upon to do. This emerges from the lack of basic due process obligations such as transparency, fairness, proportionality, and appeal that typically accompany public adjudicative roles such as the assessment of whether a statement

---

[67] *Mckinney v. University of Guelph*, [1990] 3 S.C.R. 229 (S.C.C.), at 261-262, per La Forest, J.,:

> … the *Charter* is essentially an instrument for checking the powers of government over the individual…The exclusion of private activity from the *Charter* was not a result of happenstance…Government is the body that can enact and enforce rules and authoritatively impinge on individual freedom. Only government requires to be constitutionally shackled to preserve the rights of the individual. Others, it is true, may offend against the rights of individuals. This is especially true in a world in which economic life is largely left to the private sector where powerful private institutions are not directly affected by democratic forces. But government can either regulate these or create distinct bodies for the protection of human rights and the advancement of human dignity.

[68] In *BMG Canada Inc. v. John Doe*, [2005] 4 F.C.R. 81 (F.C.A.), for example, at para. 39 the Federal Court of Appeal described its long standing expertise in balancing competing rights such as privacy and intellectual privacy enforcement. As note above (*supra* note 63), CIRA, a private corporation, attempts to strike that same balance through its terms of use.

[69] S.N. Hamilton, "Made in Canada: A Unique Approach to Internet Service Provider Liability and Copyright Infringement", *In The Public Interest*, M. Geist, Ed., (Toronto: Irwin Law Inc., 2005) 285 at 300.

[70] See, for example, *Cuttell*, *supra* note 62 at para. 79-80:

> I agree with Justice Wilkins that recognizing some degree of privacy in subscriber information is good public policy…However, it appears that Bell, Telus, Rogers and Shaw all have contracts requiring that their subscribers agree to disclosure of subscriber information in certain situations, suggesting that a continuing expectation of privacy may be unreasonable in light of some contracts. *Therefore, it may be that in most cases, the issue of whether there is a reasonable expectation of privacy in subscriber information will be resolved by the contract between the parties…In short, it means that the safeguard of an independent judicial arbiter will no longer be available to assess, in advance, whether the individual's right to privacy should give way to the law enforcement goals of the state* [emphasis added].

See also proposed Bills C-46 and particularly C-47, intended to modernize Canada's lawful investigative techniques: Bill C-46, *Investigative Powers for the 21st Century Act*, 1st sess., 40th Parl., 2009, online: Parliament of Canada <http://www2.parl.gc.ca/content/hoc/Bills/402/Government/C-46/C-46_1/C-46_1.PDF>; Bill C-47, *Technical Assistance for Law Enforcement in the 21st Century Act*, 1st sess., 40th Parl., 2009, online: Parliament of Canada <http://www2.parl.gc.ca/content/hoc/Bills/402/Government/C-47/C-47_1/C-47_1.PDF>.

is 'defamatory' or whether a work infringes copyright or not. Further, when adopting policy positions, such adoption is often an industry wide phenomenon in a crowded industry, severely limiting any possibility for a market response.[71] This is also the case for less essential services with broad and heavily invested user bases that are not readily able to pick up and leave.[72]

This lack of capacity to effectively balance and carry out public interest objectives should be troubling given the increasing extent to which individual actions are subject to private intermediary decisions of this nature. It is especially troubling where values enshrined in the *Charter*, values such as privacy and free expression, are essentially "resolved by the contract between the parties."[73] when permitted to override values enshrined in our *Charter*. As noted by La Forest, J., in *Godbout v. Longueil (City)*, narrowing the scope of *Charter* protections in this manner would be:

> …to say the least, undesirable. Indeed, in view of their fundamental importance, Charter rights must be safeguarded from possible attempts to narrow their scope unduly or to circumvent altogether the obligations they engender.[74]

It is CIPPIC's position that the government has an obligation to ensure that the proper balance is struck between competing interests when private organizations take on public-like roles that have sweeping impact on the lives of Canadians – particularly where these impact on *Charter* values or where such entities act to deprive Canadians of access to a judicial resolution of private rights.[75] In particular, the government should examine means of instilling mechanisms to ensure the level of control and surveillance available to intermediaries is not used in a manner so as to impact detrimentally on *Charter* values. This objective can be furthered by applying due process and proportionality obligations on intermediaries when such entities take on public roles. In addition, the government can begin to examine its own policies and use caution and restraint when relying on private intermediaries to achieve public policy objectives, whether through legislative or co-regulatory means.

While in some cases, such practices may be warranted, in others extreme caution should be exercised, particularly when attempting to enforce sweeping surveillance agendas. When doing so, the government must ensure that the appropriate safeguards are in place. An aspect of this would require some differentiation between intermediary actions of a public and private character. Courts can provide some guidance on this.[76] Overall, CIPPIC believes that such

---

[71] *Cuttell*, *supra* note 62 notes at paras. 79-80 that all the major ISPs in Canada have made a joint decision do extinguish any reasonable expectation of privacy and accompanying s. 8 protections for their Canadian customers.
[72] See *Spar* D. Boyd, "Facebook is a Utility; Utilities Get Regulated", *Apophenia*, (15 May 2010), online: Apophenia <http://www.zephoria.org/thoughts/archives/2010/05/15/facebook-is-a-utility-utilities-get-regulated.html>.
[73] *Ibid*.
[74] *Godbout v. Longueil (City)*, [1997] 3 S.C.R. 844 (S.C.C.), at para. 48.
[75] See also generally, M. Pavlovic, "iConsumers' Access to Justice", Centre for Law, Technology and Society Torys Lecture Series, (10 March 2009), online: Center for Law, Technology and Society <http://www.techlaw.uottawa.ca/en/list/programs/technology-law-podcast-website/> (audio recording).
[76] In *Greater Vancouver Transportation Authority v. Canadian Federation of Students – British Columbia Component*, [2009] 2 S.C.R. 295 (S.C.C.), Deschamps, J. described this character at para. 16 as such:

> If an entity is not itself a government entity but nevertheless performs governmental activities, only those activities which can be said to be governmental in nature will be subject to the *Charter*.

potential issues should be addressed by the government proactively so as to avoid the need to impose blunter, less tailored solutions.[77]

V. Reconciling Privacy and Data Protection

Theme:	*Capacity to Innovate Using Digital Technologies*
Discussion Questions:	• *What would a successful digital strategy look like for your sector?* • *Are there new legislative/policy changes needed to deal with emerging technologies?* • *How can Canada use its regulatory and policy regime to promote Canada as a favourable environment?*
Recommendations:	**8. Consider a privacy-specific Charter or Bill of Rights as a means to reconcile approaches to privacy, demonstrably strengthen Canadian commitments to the importance of privacy, and best address the increasing overlap of public and private organizations in the collection, use and disclosure of personal information.**

The tension between notions of privacy as a human right and privacy as data protection is long-standing and ongoing. In 1977, when Canada first moved to legislate regarding privacy, it did so using the vehicle of the Canadian Human Rights Act. These Provisions[78] covered information on natural persons which was held by the federal government and had been used in making decisions about the individual concerned. Although this Part of the Act is no longer in force, the decision to use the vehicle of the Canadian Human Rights Act is a significant one, underscoring notions of human dignity which are inextricably tied to privacy. Later, in 1983, Canada enacted both the *Access to Information* and *Privacy Act*s, regulating public sector bodies' collection, use and disclosure of information and replacing the CHRA provisions.[79]

Although this resulted in coverage of public sector bodies, discussions of whether and how to regulate private sector entities was unresolved. While Canada did sign on to the OECD Guidelines in 1984, other than that there was little government move towards a private sector privacy apparatus, and what private sector privacy did exist came from voluntary industry specific codes.[80]

---

[77] Professor Katherine Swinton, cited with approval by McIntyre, J., in *R.W.D.S.U. v. Dolphin Delivery*, [1986] 2 S.C.R. 573 (S.C.C.), makes this point in stating that proactive regulation is preferable to *Charter* obligations:

> Moreover, in considering whether the Charter should be directly applicable, the courts should bear in mind its drawbacks as a method of dealing with private action and the advantages of leaving the regulation of such conduct to human rights legislation or other legal controls. Legislation can be tailored to deal with the tension between privacy rights and equality or that between freedom of expression and prohibition of hate literature. It can expressly limit the applicability of equality guarantees to services or to areas open to the public, or specify the right to set bona fide job qualifications.

[78] Part IV of the *Canadian Human Rights Act*, S.C. 1976-77, c. 33.; Part IV of the *Canadian Human Rights Act* was repealed (S.C. 1980-81-82-83, c. 111 (Sch. IV, s. 3)) and replaced by the *Privacy Act* (S.C. 1980-81-82-83, c. 111, Sch. II).

[79] See *Spar* L.R. Shade, "Privacy" in M. Raboy and J. Shtern, *Communicating Rights and the Right to Communicate in Canada: Media Divides*, (Vancouver: UBC Press, 2010) at 184.

[80] For instance, credit reporting legislation enacted in the 1980s, granted consumers the right to access and correct their credit information. In an other sector, the Canadian Bankers Association adopted a model Privacy Code for individual customers in 1990 which was built on OECD Guidelines. A number of the chartered banks also developed their own individual codes.

By the 1990s, however, it was clear that the proposed European Union Directive on the Protection of Personal Data would substantially change the landscape. Of particular concern to government and private industry were the standards imposed in that document regarding transborder flows of data. The draft of the Directive circulated in the mid-1990s stated that transfer of data to a third country would only be permitted where that third country offers an adequate and recognized level of data protection. This raised fears of business relationships between European countries and Canada being blocked on the grounds that no adequate level of protection for personal data was provided. The draft also suggested that adequacy would be measured with regard to the nature of the data, the purpose and duration of the processing operation, the existence and scope of the general and sectoral data protection legislation in place, and any professional rules or Codes that applied. This galvanized a move towards some form of private sector regulation, with the Canadian Standards Association moving to develop and draft a Model Code. The intent was to develop a national voluntary code which would become the cornerstone of a national voluntary compliance framework which would in turn guide and influence institutions to establish codes of standards particular to their own environments. The Model Code was successfully completed and released in 1996.

Although the private sector movement towards a data protection approach was ongoing, the human rights-based protection of privacy was not overlooked. Beginning in 1996, the House Standing Committee on Human Rights and the Status of Persons with Disabilities began to explore the impact of (new) technologies on human rights. In 1997, they moved towards exploring the notion of privacy as a fundamental human right, researching the issue in a multiplicity of ways, including consulting with experts, and touring the country for public consultations. This resulted in an April 1997 report which not only provides an overview but proposes a privacy Charter right as a means to address the issue.

In January 1998 Industry Canada and the Department of Justice released a consultation paper entitled "The Protection of Personal Information – Building Canada's Information Economy and Society" which signalled the beginning of a move towards addressing the issue legislatively rather than relying on self-regulation. This consultation ultimately resulted in the *Personal Information Protection and Electronic Documents Act*, which received royal assent on 13 April 2000 and, as of 1 January 2004, is fully in force, applying to all personal information collected, used or disclosed in the course of commercial activities by all private sector organizations. It also applies to the personal information of employees of federal works, undertakings or businesses (FWUBs).

Understanding this history is absolutely integral to understanding PIPEDA. The recognition of the need for the law appears to have come (at least in part) from concern about maintaining and facilitating Canada's international trading relationship. The law was enacted under the federal trade and commerce power, and focuses primarily on commercial activities. Finally, the business involvement in the development of the CSA Code, which forms the backbone of PIPEDA creates a situation with an extremely unusual degree of private sector involvement in the actual drafting of the law.

This unusual degree of private sector involvement is increasingly the rule rather than the exception when it comes to privacy in Canada in both the public and private sectors. In the public sector, government is increasingly moving towards deputization of private industry as personal information collectors, a strategy which moves personal information collection, use and disclosure not merely from the public to private sector, but indeed right outside the purview of legislation at all. That is, by using private industry as their agents, the public sector can avoid the collection of personal information being governed under the *Privacy Act*, and by legislatively authorizing the collection by private organization(s) and transfer to the State, the private organizations are brought under the s. 7 exceptions in PIPEDA.

As private and public spheres of privacy increasingly overlap, both incidentally and through designed deputization, it becomes increasingly important that there be stronger protections and remedies for personal information and privacy violations available. As such, it may well be time to return to some notion of privacy as a human right.

It might be suggested (as it has been in the past) that a right of privacy be added to Canada's *Charter of Rights and Freedoms*. There are, however, a number of reasons such a strategy is not desirable, nor necessarily workable. First of all, the Charter applies only to government action. As such, it is not an effective way to address the increasing privatization of law enforcement and security, from whence much of the overlap springs. Secondly, the Charter is already held to contain some (limited) privacy rights, notably in s. 2(b), s. 7 and s. 8 – these rights are established and understood, and could well be invalidated or skewed by the introduction of a new right of privacy. Finally, and most practically, to add a new right to the Charter would be a constitutional amendment – an unlikely to be successful, contentious, time-consuming and expensive process to be avoided unless absolutely necessary.

Perhaps, rather than attempting to create a new constitutional right, the existing legislation could or should be amended. While PIPEDA does have a mandatory review built into the statute, the Privacy Act has not been amended since its introduction in 1983! Certainly it is important – necessary even – that both these statutes be updated to be contemporary and to take account as much as possible of evolving technological capacities. Indeed, CIPPIC notes that the government has been eager to update its own investigative powers so as to keep up with these same technological changes.[81] Certainly privacy protections merit the same. Nevertheless, updating the acts will not necessarily address the overlap of private and public sector interests which concerns CIPPIC, since the existing legislative scheme treats each sphere as separate.

This brings us, finally, to the notion of some kind of Privacy Charter. This was originally proposed in 1997 in "Privacy: Where Do We Draw the Line", the report of the House of Commons Standing Committee on Human Rights and the Status of Persons of Disabilities, but was not adopted legislatively. It may be time to revisit this approach. The creation of some kind of privacy-specific Bill serves many purposes – it can reconcile the public and private interests; it prevents private arrangements between the State and private sector organizations that take information transactions effectively outside the realm of privacy legislation, and it could constitute a policy statement about government commitment to privacy even as it functioned to

[81] Public Safety Canada, "Technical Assistance for Law Enforcement in the 21st Century Act", *Newsroom*, (18 June 2009), online: Public Safety Canada <http://www.publicsafety.gc.ca/media/nr/2009/nr20090618-1-eng.aspx>.

enhance privacy itself. In addition, such strong privacy guarantees are sure to instil greater confidence in the digital marketplace.

VI. Updating Canada's Private Sector Legislation

Theme:	<u>*Capacity to Innovate Using Digital Technologies*</u>
Discussion Questions:	• *What would a successful digital strategy look like for your sector?* • *Are there new legislative/policy changes needed to deal with emerging technologies?* • *How can Canada use its regulatory and policy regime to promote Canada as a favourable environment?*
Recommendations:	**9. Amend PIPEDA to include order making powers as well as to establish the possibility of statutory damages in certain circumstances;** **10. Amend PIPEDA so as to allow organizations to file complaints;** **11. Add cost immunization for *bona fide* applicants under s. 14;** **12. Explore the possibility of imposing PIA obligations on private sector organizations;** **13. Clarify that blanket consent clauses are unacceptable under PIPEDA;** **14. Repeal proposed s. 7(2) of Bill C-29 and instead adopt a holistic approach to employee consent more capable of protecting the individual dignity that is at high risk in employee-employer relationships;** **15. Amend PIPEDA to provide stronger, categorical protections for privacy of minors;**

A. Compliance and Enforcement Powers

In Canada, of the four bodies that are charged with ensuring Canadians' data is protected, only our federal private-sector privacy legislation, the almost decade-old PIPEDA, does not provide for order-making powers. It employs an ombudsman-model for the Privacy Commissioner, which leads to the issuance of recommendations on how parties should act to comply with PIPEDA. Substantially similar provincial agencies in BC, Quebec and Alberta have order making powers.

At one side of the spectrum, a lack of enforcement powers encourages lawlessness and not doing what the OPC wants. Copyright laws are not recommendations, why should privacy laws be?

On the other end of the spectrum is a model of new governance which is more conducive to dialogue and working together to achieve the same goals an enforcer would have - compliance with PIPEDA, but without having to use the threat of sanctions to meet those ends. This latter approach is based on the premise that, lacking the threat of sanction, organizations will enter into more open relationships with the Privacy Commissioner and be more willing to approach proactively for assistance where privacy issues emerge.

This theory is that solutions that are voluntarily entered into, will be self-regulating and enduring. The advocates of this theory criticize the order-making model as they contend it requires a more adversarial/litigious and less flexible/mutually productive outlook. They contend it is less

effective to resolving privacy disputes. As consensus is essential to public interest disputes, an adversarial imposition of settlements delineates between victors and losers and deprives all parties of resources that could be better invested.[82]

Perhaps the OPC is sometimes in the middle, not being completely confident in one side or the other, because the advocates of enforcement powers should come from the public at large, as oppose to the hand that will be granted the power. As Canada's internet policy public interest group, CIPPIC will gladly take the lead. Further, the OPC may want to rely, and commendably so, on the founding reasons for why PIPEDA began with an ombuds model.

To preface any criticism on the efficiency of this model in 2010, PIPEDA's enforcement roots must be understood. PIPEDA is not a typical regulator of government legislation.

In the Privacy Commissioners publication October 2005 publication, "Cherry Picking Among Apples and Oranges: Refocusing Current Debate About the Merits of the Ombuds-Model Under PIPEDA" Jennifer Stoddart pointed out key points about the ombuds-model as it relates to PIPEDA.[83]

For literally centuries, the ombuds-model has been practiced in accordance with its roots: being "focused first and foremost on the protection of certain values, values of equity and accountability."[84]

Ombudsmen provide a chance for ordinary people, those typically without the power, to be heard and to get fair treatment from those with power.[85] Before PIPEDA, the Privacy Act had an ombuds-model.[86] Upon enacting PIPEDA, this ombuds-model was maintained.

It has long been CIPPIC's position that the Commissioner requires order making powers if PIPEDA is to inspire the proper incentives in organizations. While some larger players may, under an ombuds-model, develop more positive relationships with the Commissioner's office and may at times be willing to cooperate without any threat of sanctions, this is certainly far from the norm.[87] The majority of data controllers do not proactively comply with PIPEDA requirements in numerous ways, perhaps knowing that the costs of non-compliance are likely to be low.[88]

---

[82] Stephen Owen, "The Expanding Role of the Ombudsman in the Administrative State" (1990) 40 UT.L.J. 670 at 684.
[83] J. Stoddart, "Cherry Picking Among Apples and Oranges: Refocusing Current Debate About the Merits of the Ombuds-Model Under PIPEDA" *Office of the Privacy Commissioner of Canada*, (21 October 2005), online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/information/pub/omb_051021_e.cfm>.
[84] Nathalie Des Rosiers, "Balance and Values: The Many Roles of an Ombudsman", presentation delivered at the Annual Conference of the Forum of Canadian Ombudsman, April 2003 at 3.
[85] Carolyn Steiber, "57 Varieties: has the Ombudsman Concept become Diluted?" (2000) 16(1) *Negotiation Journal* 49 at 56.
[86] *Lavigne v. Canada (Office of the Commissioner of Official Languages)* [2002] 2 S.C.R. 773.
[87] CIPPIC, "Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?", CIPPIC, (April 2006), online: <http://www.cippic.ca/documents/bulletins/compliance_report_06-07-06_%28color%29_%28cover-english%29.pdf>. This study rated the privacy practices of 64 retailers across four distinct metrics and found widespread non-compliance in all four areas, in large organizations as well as small.
[88] *Ibid*.

In many cases, once the privacy violation has occurred, it is often difficult to undue the resulting harm.[89] With the costs so high for consumers, it is perfectly justified and essential to provide the Commissioner with the option of imposing equally high costs onto organizations that fail to comply with PIPEDA.

Without strong economic incentives in the form of penalties, compliance will remain fleeting and, where present, will typically extend only so far as convenient. Further, in CIPPIC's view, providing the Commissioner with the option of imposing penalties does not deprive her of adopting less adversarial approaches. It merely provides the Commissioner with an additional and necessary tool in her attempts to ensure compliance with PIPEDA.

In this respect, PIPEDA must be updated so as to better ensure compliance. This requires order making powers for the Commissioner so her findings cannot be ignored, it requires the availability, in some circumstances, of statutory damages, it requires that the Act be amended to recognize that organizations can file complaints on behalf of the public interest, and s. 14 should be amended to provide cost immunity for *bona fide* and responsibly carried out federal court applications. The government should explore the possibility of creating privacy impact assessment mechanisms or obligations for private sector entities so as to ensure continued and *forward looking* compliance in the introduction of new technologies.

B. Clarify that blanket consent is not acceptable

PIPEDA is purportedly a tool of data protection intended to allow nuanced and granular informational self-determination to individuals, while still facilitating reasonable/necessary collection, use and disclosure of personal information by organizations. Unfortunately, in an attempt not to overly fetter themselves too many organizations list every possible use or disclosure to which personal information might be subject, ultimately overloading the individual with information such that (at least arguably) her ability to choose meaningfully is compromised. In order to facilitate the kind of nuanced and comprehensible information and consent model envisioned in the Act, it is important that the importance of nuanced consent processes be emphasized.

In its original consultation paper on Privacy Act amendments, the Office of the Privacy Commissioner of Canada problematized "consent" in a number of different ways. Among them, it suggested a (re)consideration of the notion of consent in such a way that "blanket consent"[90] was explicitly refused as an acceptable model. Although the suggestion was not incorporated into the final submission, nor has it formed part of the ongoing PIPEDA reform discourse, this should not be taken to indicate the idea is without merit.

As Barrigar et al have argued "[t]aken altogether, the consent provisions in *PIPEDA* strongly suggest that consent acts like a "license" that permits some *limited* collection, use, or disclosure. Thus, the consent given to an organization to use an individual's personal information is

---

[89] J. McNish and O. El Akkad, "Facebook Warned it's not in compliance", *Globe and Mail*, (26 May 2010), online: <http://www.theglobeandmail.com/news/technology/facebook-warned-its-not-in-compliance/article1582155/?cmpid=rss1>.

[90] The notion of "blanket consent", of course, is a consent clause drafted carefully and broadly enough that the consent given arguably permits a wide (virtually unlimited) range of future collections, uses and disclosures.

necessarily restricted and *does not* give the organization ultimate control over personal information in perpetuity."[91]

CIPPIC contends that PIPEDA language is already clear enough on this point, with various provisions addressing this issue -- *PIPEDA* Principle 4.2.2 for instance says that consent is only given for the purposes specified. Under Principle 4.4 these purposes must be appropriately limited, and under Principle 4.5 all uses or disclosures require consent and should be documented as *per* Principle 4.5.1. Almost any new purpose beyond those already specified requires new consent, as set out in Principle 4.2.4. Taken together, these provisions indicate a strong understanding of consent as an ongoing act of agency rather than an isolated all-or-nothing moment or document.[92]

Nonetheless, CIPPIC encourages the government to recognize explicitly in the Act that blanket consents are not acceptable. Consent cannot provide the requisite level of granularity nor can it be meaningful if individuals are asked to forfeit all of their future controls over their information in one click.

C. Holistic analysis of employee consent

Bill C-29, introduced in the House of Commons in June 2010, would amend PIPEDA to add, s. 7.2, an exception that would move the statute from a consent to a notice standard for the collection, use or disclosure of information about an employee or potential employee of a federal work, undertaking or business where the information is necessary to establish, manage or terminate an employer/employee relationship.

Of substantially similar private sector statutes in Canada, both the British Columbia and Alberta Personal Information Protection Act(s) contain within them similar provisions dealing with the personal information of employees, although these are limited by an internal reasonableness standard. Quebec does not distinguish employee information at all.

Employee privacy and how best to address it is a contentious question – while criticisms have been levelled at the consent model for failing to recognize the potential impact of power differentials and economic coercion in shaping employee responses, criticisms may also be levelled at any suggestion that by virtue of employment the personal information of an individual is entitled to a lessened standard of protection. Regardless of where one falls on the C-29 provisions, the fact that employees are in a precarious position with regard to consent can not be argued. Given this, CIPPIC encourages a nuanced and holistic approach to assessing privacy-invasive practices and their impacts within the employment sphere. Such an approach must necessarily look not only at the practice itself, but also at the workplace. This is consistent with

[91] Kerr, Ian R., Barrigar, Jennifer, Burkell, Jacquelyn and Black, Katie, "Soft Surveillance, Hard Consent", Personally Yours, Vol. 6, pp. 1-14, 2006. at 6, online: Social Science Research Network: <http://ssrn.com/abstract=915407>.

[92] A useful example of the problems with blanket consent clauses can be found by reviewing the ongoing privacy issues with Facebook. As Facebook has changed functionalities – from college/university students only to open registration, from private network to one publicly indexed by search engines, etc – information sharing too has changed. However, rather than adhere to the original intent/expression to govern use and disclosure of the information, Facebook continues to reset user privacy settings, incorporating ever-more-open default settings.

the Office of the Privacy Commissioner's own submission on PIPEDA review in which it emphasized the importance of a dignity analysis, explaining that:

> …instead of looking at a complaint relating to intrusions flowing from voice prints, location tracking or video surveillance, the OPC should have the authority to look beyond the specific application of the technology to make an effective assessment of the intrusion on the employee's dignity in the work environment as a whole. It could also be argued that we would be more accurately assessing the balance that the legislators intended in the purpose clause if we were to assess these broader consequences.[93]

Although the Committee did ultimately recommend that the British Columbia, Alberta and Quebec models be considered as part of the project of addressing the position of employees of federal works, undertakings or businesses under PIPEDA[94], these recommendation failed to address the specific concerns raised by the Privacy Commissioner with respect to the need for a dignity analysis, nor is there any such language in the proposed amendment.

CIPPIC wishes to add its voice to that of the Privacy Commissioner in emphasizing the need for a privacy analysis that is focussed on protecting the dignity and autonomy of the individual rather than merely on regulating the flow of information. Central to such a position must be a focus on the impact of a practice or technology *in all the circumstances*. In this regard, the changes proposed by Bill C-29 with respect to employee information handling practices not only fail to implement the OPC's recommendations but in fact fail to adequately protect the personal information of employees.

D. PIPEDA Protection for Minors

Currently, PIPEDA makes no explicit distinction between adults, children and "minors". Although the Note to Principle 4.3 does make some acknowledgement of the difficulty of getting consent from minors, it should be noted that s. 2(2) of PIPEDA clarifies that such Notes are not part of PIPEDA for the purposes of application or interpretation. Further, although the Statutory 5-year Review of PIPEDA did recommend amending PIPEDA to address this issue (Recommendation 15)[95], a recommendation that has since been endorsed in the Government Response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics,[96] such an amendment has yet to be introduced. Bill C-29 does purport to address this issue by adding s. 6.1 to PIPEDA which would read:

For the purposes of clauses 4.3 to 4.3.8 of Schedule 1, the consent of an individual is only valid 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.

---

[93] Online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/parl/2007/sub_070222_e.cfm#004>.
[94] Recommendation 5: Fourth Report of the Committee on Access to Information, Privacy and Security at 12.
[95] Online: Parliament of Canada <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=2891060&Language=E&Mode=1&Parl=39&Ses=1>.
[96] Government Response to the Fourth Report of the Standing Committee on Access to Information Privacy and Ethics, online: Industry Canada <http://www.ic.gc.ca/eic/site/ic1.nsf/eng/00317.html>.

While this is helpful, the capacity to consent meaningfully is not the only issue that necessitates greater attention and care to the privacy of children's personal information. Additionally, cognitive science suggests that many (if not most) individuals aren't fully cognizant of the consequences of the collections, uses and disclosures to which they consent, or if they are, are focussed more on short-term gains than on the possibility of long-term losses.[97]

This is not to say that there is a total vacuum of law in Canada with regard to minors and consent – a number of sources have provided input on how the issue of capacity should be treated in various contexts. The common law deems minors (those under 18 years of age) to lack legal capacity and thus requires an adult to speak for them in courts, make decisions for them, and generally act on their behalf in exercising legal rights. At the same time, however, there has evolved a common law recognition (which has been codified in legislation in some provinces, at least with respect to medical procedures) of at least the possibility of child (especially older adolescent) agency in some circumstances. This doctrine of the "mature minor" has primarily been articulated in situations dealing with consent to medical treatment.

One approach to the question of the "mature" minor has been to build into statutes a graduated presumption of ability to consent. Where Canadian law has traditionally treated individuals over the age of majority as capable of informed consent in the absence of proof to the contrary, some statutes are making the age of majority standard more flexible. For instance, the *Medical Consent of Minor's Act*[98] sets up a system where (1) minors who are 16 or older are considered to have the same right/ability to consent as if they had attained the age of majority and (2) a minor who is not yet 16 may give consent where in the opinion of a medical practitioner or legally qualified dentist (a) the minor is capable of understanding the nature and consequences of a medical treatment, and (b) the medical treatment and the procedure to be used is in the best interests of the minor and his continuing health and well-being.

As well, the federal government has addressed the issue of consent in the *Criminal Code of Canada*. In Part V (Sexual Offences, Public Morals and Disorderly Conduct), the Code seems to set the bar at age 14, with some limited exceptions for children 12 or 13. Similarly, the federal *Young Offender's Act* distinguishes between children up to age 12, and individuals between the ages of 13-18, with the Act applying only to the latter category.

Nor is law the only avenue from which guidance on appropriate policies and approaches to advertising to children can issue. Indeed, a number of organizations have codes and policies dealing with this issue and have done so specifically in the context of privacy and marketing.

Advertising Standards Canada, for instance, has a policy document entitled "The Broadcast Code for Advertising to Children"[99] which defines children as those under age 12 and deals with issues

[97] Jennifer Barrigar, Ian Kerr, Jacquie Burkell "Let's Not Get Psyched Out of Privacy: Reflections on Withdrawing Consent to the Collection, Use and Disclosure of Personal Information", online: Social Science Research Network <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1303184>.
[98] *Medical Consent of Minor's Act*, R.S.N-B, c. M-6.1.
[99] Advertising Standards Canada, "The Broadcast Code for Advertising to Children", online: Advertising Standards Canada <http://www.adstandards.com/en/clearance/Childrens/broadcastCodeForAdvertisingToChildren.pdf>.

such as factual representation; appropriate content; avoiding undue pressure; scheduling; and social standards.

A particularly nuanced code has been developed by the Canadian Marketing Association.[100] Rather than focussing only on those under 12 or seeking to deal with everyone under the age of 18 as a homogenous group of desires and competencies, the CMA distinguishes between "children" under the age of 13 and "teenagers" between the ages of 13-16.

For children, the CMA Code stipulates that any personal information being collected, used or disclosed requires the opt-in consent of a parent or guardian. Between 13 and 16, teenagers are considered competent to consent to the collection and use of their own contact information, but any disclosure of that contact information requires the opt-in consent of the parent or guardian. As for personal information beyond contact information, until age 16 the collection, use or disclosure of this information will still require the opt-in consent of the parent or guardian. Finally, for teenagers over 16 but under the age of majority, teenagers are considered competent to consent to the collection, use or disclosure of their own personal information. In every case, where the teenager or parent or guardian withdraws or refuses consent for a collection, use or disclosure of the personal information, marketers are required to immediately delete the information from their database(s).

A final suggestion is made by PIAC and endorsed by the Working Group of Canadian Privacy Commissioners and Child and Youth Advocates in a recent report.[101] PIAC calls for a solution similar to that of the CMA, but adds a general prohibition below the age of thirteen, while extending the period where opt-in adult consent is required to cover ages 13-15, and requiring opt-in consent from the teen for ages 15-16 (or to the age of maturity). CIPPIC recommends that PIPEDA be amended to include requirements tracking PIAC's recommendations.

[100] Code of Ethics and Standards of Practice, at sections "K" and "L", online: Canadian Marketing Association <http://www.the-cma.org/?WCE=C=47|K=225849#13>. This code is also of interest since the CMA's Code of Ethics and Standards of Practice" is mandatory for all members.

[101] Working Group of Canadian Privacy Commissioners and Child and Youth Advocates "There Ought to Be a Law: Protecting Children's Online Privacy in the 21st Century", (19 November 2009), at 17, online: New Brunswick Canada <http://www.gnb.ca/0073/PDF/Children%27sOnlinePrivacy-e.pdf>.

VII. Updating Canada's Ancient Public Sector Privacy Protections

Theme:	*Capacity to Innovate Using Digital Technologies*
Discussion Questions:	• *What would a successful digital strategy look like for your sector?* • *Are there new legislative/policy changes needed to deal with emerging technologies?* • *How can Canada use its regulatory and policy regime to promote Canada as a favourable environment?*
Recommendations:	**16. Undertake a long overdue complete overhaul of the Privacy Act;** **17. Amend the Privacy Act so as to limit collection of personal information to those instances where the purpose for the collection is directly related to and necessary for a program or operation of the collecting agency;** **18. Limit secondary uses and disclosures of personal information by and between government agencies to those directly related to and necessary for the purpose for which the information was initially collected;** **19. In the alternative, require government agencies to notify Canadians when their data will be used or disclosed for secondary purpose except where counterproductive;** **20. Add an obligation on government agencies to take reasonable measures to safeguard personal information of users;** **21. Add a breach notification obligation;** **22. Modify the definition of 'personal information' so that it is not limited to what in recorded form;** **23. Provide the Commissioner with order making powers under the Privacy Act;** **24. Expand s.41 to cover all violations of the Act, not merely access to information denials;** **25. Add statutory damages for violations of the Act;** **26. Add some form of statutory protection against outsourcing Canadian personal information to foreign jurisdictions that lack sufficient privacy protections;**

The Privacy Act (the 'Act') - enacted in 1983[102] - was intended to create a fool-proof privacy framework to govern the federal public sector's dealings with personal information of Canadians in an age without the Internet and other advanced digital technologies. The technologies of today provide the government with continually increasing capacity to collect, manipulate, use and disclose vast amounts of Canadian's personal information. The capabilities of these technologies combined with constant political pressure, create a remarkably high risk for abuse. The Act is not sufficient to address issues of abuse or issues involved with emerging technologies. The Act also does not correspond to the actions government can take today with respect to personal data of Canadians. Further, the privacy frameworks of the private sector and many provincial public sectors offer far stronger and more sophisticated protections than the Act.

[102] Canada, Standing Committee on Human Rights and the Status of Persons with Disabilities, *Privacy: Where do we draw the line?* (Ottawa: Public Works and Government Services of Canada, 1997) at 25.

Both the House of Commons Standing Committee on Access to Information, Privacy and Ethics and the Office of the Privacy Commissioner agree the Act is completely outdated.[103] The government's response stated the public and private sector are different, policies are an appropriate substitute for amendments, information sharing with foreign states protects the health and welfare of Canadians and the Act along with the *Charter* sufficiently covers the Privacy Commissioner's concerns.[104]

We agree, the public sector is different from the private. The public sector operates for and in the public interest of Canadians. As such, it logically follows that privacy protections in the public sector must be noticeably stronger than private sector data protections. With the onslaught of new technologies being released daily, the Act is neither flexible enough to deal with privacy concerns related to these technologies nor restrictive enough to regulate current government practices involving personal data.

The government's repeated decisions to leave the Privacy Act alone[105] must end. Legislators need to step up protections surrounding personal information of Canadians held by government.

Updating the Act to correspond with today's digital society and the gravity of potential issues is crucial. Like building a house, a solid foundation is necessary to build a consumer-friendly digital economy. Confidence in the economy must, however, accompany substantive privacy guarantees – Canadians *do* care about their privacy and no less so where it is at risk from government access.[106] This solid foundation includes a strong Canadian legislative framework for privacy protection in the federal public sector.

We call for a complete overhaul of the Act. The recommendations below are quick and temporary fixes that can be used in the meantime until the Act undergoes a thorough and detailed examination by Parliament and is re-created. The recommendations offer a survey of the Act's prominent issues. They include modifying the current system for collection, use and disclosure of personal information, creating protections for online disclosures, the need to add security standards and breach notification requirements, expanding the definition of 'personal information', providing better channels for enforcement and review and reconsidering data sovereignty as a global issue.

A. Collection, Use and Disclosure

i. Collection

The Act allows federal government to collect personal information if it relates directly to a program or activity of the institution. As a result, individuals are susceptible to giving unnecessary personal information to federal government agencies, like the Canada Revenue

[103] "Government: Update Investigative Techniques, Not Privacy" (17 October 2009), online: Digital Agenda <http://www.digitalagenda.ca/police_surveillance/Contradictions>.
[104] Government Response to Canada, Standing Committee on Access to Information, Privacy and Ethics, *The Privacy Act: First Steps Toward Renewal*, (Ottawa: House of Commons, 2009).
[105] See Government Response to Canada, Standing Committee on Justice and Solicitor General, *Open and Shut* (Ottawa: Public Works and Government Services of Canada, 1987) and to Standing Committee on Human Rights and the Status of Persons with Disabilities, note 1.
[106] EKOS Research Associates, "Revising the Privacy Landscape a Year Later" Office of the Privacy Commissioner of Canada, March 2006, online: <http://www.priv.gc.ca/information/survey/2006/ekos_2006_e.cfm>.

Agency. The Act should restrict collection of personal data by the government to only necessary data for properly implementing their program or activity. This reform acknowledges that Canadian privacy is valued and follows private and provincial public sectors of Canada.

The 'Collection of Personal Information' provision, s.4 of the Act, allows government institutions to collect personal information of individuals if the information relates directly to an operating program or activity of the institution.[107] There is no consent requirement.

Section 4's standard for collecting personal information is so remarkably low it compromises privacy protections for Canadians. Section 4 places no restrictions on what data government institutions can collect. The only requirement is the data collected is 'directly related' to one of the institution's many programs or activities. Also, 'operating program or activity' is merely defined as that related to an 'administrative purpose' in the Act.[108] This offers the government a lot of lee-way for procuring highly-sensitive personal data. Government institutions only need to show they are collecting personal information for an 'administrative purpose'. It doesn't matter if the information is unnecessary for fulfilling the program or activity's purpose.

The standard for collecting personal information should include a 'necessity test'. The 'necessity test' would ensure government institutions can only collect personal information if it is 'necessary for' the institution's operating program or activity. The restriction we propose is reasonable and establishes a more proportionate balance between the interests of government and the privacy interests of Canadians. The 'necessity' standard provides appropriate safeguards and recognizes that privacy in Canada is valued. Further, the privacy laws for private organizations, many provincial governments and the Treasury Board all have a necessity requirement in place for collection of personal information.

Section Recommendations:

- CIPPIC recommends s.4 of the Privacy Act be amended to mandate that "No personal information shall be collected by a government institution unless it relates directly to and *is necessary for* an operating program or activity of the institution."

ii. Secondary Use and Disclosure

The Act allows government to use personal data for secondary purposes and disclose it to secondary entities if the use or disclosure is consistent with its original purpose for collecting that data. Individuals have practically no control over their personal information once released to federal government institutions. The Act should require consent and notification and in addition place restrictions on secondary uses and disclosures. This reform would provide Canadian's with more autonomy over the use and disclosure of their personal data.

The 'Disclosure of Personal Information' provision, ss.7(a) and 8(2)(a) of the Act rely on a standard of 'consistency' with the original purpose of collection as the only limiting principle on

[107] *Privacy Act*, R.S.C. 1985, c.P-21, s.4.
[108] Barbara McIsaac, Rick Shields & Kris Klein, *The Law of Privacy in Canada*, (Scarborough: Thomson Carswell, 2006) at 3-10.

secondary uses and disclosures.[109] The Act does not even have a notice requirement for such secondary uses or disclosures.

The term 'consistent' creates a low threshold for using and disclosing information. For example, the Supreme Court of Canada affirmed that providing customs information about travellers to the Canadian Employment Insurance Commission (CEIC) in order to catch people receiving unemployment insurance outside the country is a use/disclosure 'consistent' with the Department of National Revenue's initial customs-related purpose for collection.[110]

The Federal Court of Appeal reasoned that CEIC must be able to collect information from an outside source and the numerous exceptions in s.8(2) clearly shows Parliament's intention to allow disclosure for purposes other than the original reason for collecting the information and to persons who have no connection to the disclosing institution.[111] This is problematic because individuals travelling have no control over their personal information and no choice in which government institutions can access and use their personal data. With this ruling, federal government institutions can use and disclose data with practically any other federal government institution under the guise of protecting against fraud.

Allowing secondary use and disclosure of personal data between federal government agencies and bodies completely jeopardizes the privacy of Canadians. This is exacerbated by the lack of any notice requirement in that Canadians will in many case not be given the chance to challenge secondary uses or disclosures even on the low 'consistency' standard.

Secondary uses and disclosures should only be allowed if it is 'necessary for' and 'directly related to' the institution's original purpose for data collection, or if individuals give consent to the new uses and disclosures. At minimum, the Privacy Act must require notification where such secondary uses and disclosures occur – except where such notification would be counter-productive.

Section Recommendations:

- CIPPIC recommends both s.7(a) and s.8(2)(a) of the Privacy Act be amended to require disclosure of information only when *necessary for* and *directly related to* the purpose for which the information was obtained or compiled by the institution.
- CIPPIC recommends both s.7(a) and s.8(2)(a) of the Privacy Act be amended to require notifying individuals of new uses and disclosures before the uses and disclosures not reasonably expected when the information was collected, except in cases where notice is counter-productive.

B. Security

The Act does not have provisions for taking security measures to protect personal data and does not have provisions for data breach notification to individuals. This places individuals in an extremely vulnerable position given that data breaches have become increasingly prevalent in

[109] *Supra* note 6 at ss.7(a), 8(2)(a).
[110] *The Privacy Commissioner of Canada v. The Attorney General of Canada*, 2001 SCC 89, [2001] 3 S.C.R. 905, (S.C.C.).
[111] *Supra* note 8.

recent years.[112] Firstly, government institutions should be required to take the necessary security measures to protect the personal data they collect, use and disclose. Secondly, a breach notification system must be implemented to give notice to affected individuals so as to facilitate remedial measures. These security and notification provisions provide technological protection of Canadian's personal data and provide a transparent a plan of action if and when data breaches occur.

The Act has neither provisions for security protection of data nor any breach notification system. This means there is no obligation on government institutions to secure data they collect, use and disclose. Further, there is no obligation on government institutions to notify affected individuals in the event of a breach. If a data breach within a government agency were to occur, affected individuals may never find out. This presents many privacy issues for Canadians, especially identity theft.

In the U.S., the government has suggested breach notification provisions should apply to the public and private sector.[113] The U.S. clearly recognizes that breach notifications by government institutions is just as pressing a need as breach notifications provisions for private entities – from the individual's perspective if the data is gone the data is gone.

Government institutions should be required to 1) take reasonable security measures to protect personal information from unauthorized access, use or disclosure, and 2) implement a notification system for individuals affected by security breaches exposing their personal information to potentially harmful uses. These security and notice measures provisions would ensure that security precautions are taken for personal information and allows individuals to take corrective measures by informing them of data breaches. In addition, the Act would be consistent with the private sector regarding security provisions and with countries such as the UK and the U.S. regarding breach notification provisions.

Section Recommendations:

- CIPPIC recommends the Act be amended to add a new provision requiring government institutions to take reasonable security measures to protect data from unauthorized access, use or disclosure;
- CIPPIC recommends the Act be amended to add a new provision requiring government institutions to notify affected individuals of security breaches that expose their data to third parties.

C. Definition of 'personal information'

The Act is only applicable to recordable personal information. As a result, individual's unrecorded personal information has no privacy protections against federal government institutions. The Act should define 'personal information' to include both recorded and unrecorded information. In doing so, new and emerging methods for collecting unrecorded

[112] Lloyd Borrett, "Who Suffers Most as a Result of Data Breaches? Customers, Company or Employees?" *Cfo World* (25 June 2010), online: International Data Group <http://www.cfoworld.com.au/mediareleases/10896/who-suffers-most-as-a-result-of-data-breaches/>.
[113] U.S., Bill S.139, *Data Breach Notification Act*, 109th Cong., 2009.

personal information will be subject to the same privacy protections as recorded personal information and the privacy of Canadians. This is particularly necessary with the growing ubiquity of geolocational devices.

Under s.3 of the Act, 'personal information' is defined as information about an identifiable individual that is recorded in any form.[114] Due to the Act's 'personal information' definition, there are no legal privacy protections for unrecorded personal information held by federal government institutions. This creates a considerable gap in Canada's privacy laws that is all the more likely to expand as technological advances add to the category of information capable of being collected in unrecorded format.

The Act provides federal government institutions with free reign – subject only to the *Charter* – over collection, use, manipulation and disclosure of data such as video surveillance, DNA samples of individuals and GPS and other location-based technological surveillance. With respect to biosamples, it does not even place any limitations on indefinite retention. Given the powers of government institutions to engage in extremely intrusive practices into Canadian's lives, it is imperative that the Privacy Act be applicable to all personal information, both recorded and unrecorded.

Section Recommendations:

- CIPPIC recommends to amend the definition of 'personal information in s.3 of the Act to remove 'that is recorded in any form'.

D. Enforcement and Review

The Act does not instil the Privacy Commissioner with order-making powers.[115] The Act's provisions for applying for Federal Court review are restricted to access to information refusals. Further, there are no statutory damages available. As such, individual enforcement of the Act is very difficult and there is no incentive for government institutions to adhere to the Act. The Act should give the Privacy Commissioner order-making powers, the provision for application for Federal Court Review should be open to all privacy right violations and statutory damages for cases involving harm should be legislated. These reforms will add more enforceability to the Act and ensure that privacy rights of Canadians are taken more seriously by federal government institutions.

i. Order-making Powers

The current Act does not give the Privacy Commissioner order-making powers.[116] This means the Privacy Commissioner's recommendations for collection and use of personal information are not legally binding. Order-making powers would create better enforceability of the Act for individuals who have suffered privacy violations. The Privacy Commissioner would have power to take legal action against institutions violating privacy rights of Canadians.

The Privacy Commissioner requires order-making powers. This would offer the Privacy Commissioner more clout and assist in individual enforcement of the Act. This is not out of

[114] *Supra* note 6 at s.3.
[115] *Ibid*.
[116] *Ibid*.

character with many provincial privacy laws where the provincial Privacy commissioner is endowed with order-making powers, such as the provinces of B.C. and Alberta.

Section Recommendations:

- CIPPIC recommends the Act be amended to give the Privacy Commissioner order-making powers.

ii. Review

The Act's 'Review by Federal Court' enforcement provision is limited to cases where 'access to information' requests are refused.[117] Further, for these 'access to information request' cases, individuals who wish to apply to the Federal Court to review their case must satisfy several requirements including making a complaint to the Privacy Commissioner and applying to the Court within 45 days from when the Privacy Commissioner reports the results of their investigation into the complaint. This limitation means enforcement of the Act by both individuals and the Privacy Commissioner on behalf of individuals is severely restricted.

Individuals cannot seek redress for privacy violations committed against them by government institutions, except for cases involving denied access to information requests. Essentially, government institutions can violate the privacy rights of Canadians without having to face legal consequences in most cases. As a result, the Act becomes merely an illusion of privacy protection for Canadians. Individuals have little chance, if any, of enforcing their rights. The incentive for federal government institutions to comply with the Act is negligible, as they are unlikely to be held responsible for any privacy violations.

The 'Review by Federal Court' provision should be expanded to all privacy rights including collection, use and disclosure of one's personal information. This will provide individuals with more opportunity and autonomy for enforcing their privacy rights under the Act via the Federal Court.

The proposed modification to s.41 could also act as an alternative for the federal Privacy Commissioner's order-making powers. However, this mechanism is imperfect. There is a high cost for individuals to enforce these socially significant rights through Federal court. Litigation is costly, time-consuming and the remedies issued tend not to be monetary awards. There is little incentives for Canadians to enforce their rights and many monetary risks involved in attempting to do so.

Section Recommendations:

- CIPPIC recommends the s.41 of the Act be expanded to include all privacy rights, not only access to information rights.

E. Damages

The Act does not have any provisions for statutory damages. This is another reason why there is no incentive for government institutions to follow the Act and there is weak enforceability of the

[117] *Ibid*. An individual can apply to the Federal Court for Review if their access to information request has been refused by a federal government institution.

Act by individuals. Individuals that suffer from serious privacy violations do not receive any form of compensation.

Statutory damages should be available for individuals who suffer harm from privacy violations by the government. We propose that individuals be entitled to no less than $1000 in damages and legal fees. This proposal is in accordance with the U.S. federal Privacy Act.[118] Factors for considering the 'harm' suffered in awarding damages should include embarrassment suffered, financial loss, the nature of the act and other relevant considerations.[119] The creation of statutory damages deters federal government institutions from committing privacy violations and promotes enforcement of individuals privacy rights.

Section Recommendations:

- CIPPIC recommends the Act be amended to include a statutory damages provision, where individuals who suffer harm from privacy violations by the government are entitled to up to $1000 in damages and legal fees.
- CIPPIC recommends that factors for considering the harm suffered by the individual in quantifying damages include embarrassment, financial loss, nature of the act and other relevant considerations.

F. Data Sovereignty

The Act does not have any provisions to protect personal information of Canadians transferred to foreign entities by government. This leaves Canadian data abroad open to abuse and inappropriate treatment by foreign states that do not enjoy the same privacy protections available in Canada. The Act should include safeguard provisions for Canadian personal data held abroad. This will ensure individuals enjoy Canadian privacy protections wherever their personal information resides.

Currently, the government may outsource personal information of Canadians to any country anywhere in the world without so much as notifying them. As data protections standards vary greatly across the territorial jurisdictions of the world, the Privacy Act should impose obligations on governments to at least notify Canadians of the risk to their data that such outsourcing may pose. The Act should also require government entities to consider the degree of foreign data protection offered, including potential for foreign lawful access, when deciding whether to outsource or not.

Section Recommendations:

- Amend the Act so as to provide protection against outsourcing to territorial jurisdictions with inadequate privacy protections;

[118] *Privacy Act of 1974*, Public law No. 93-579, 88 Stat.1897, 5 U.S.C. § 552a (g).
[119] These are some of the factors considered in Manitoba's Privacy Act; *The Privacy Act*, R.S.M 1987, C.C.S.M. c. P125, s.4(2).; See also *Supra* note 11.

VIII. Online Content Management

Theme:	*Digital Media: Creating Canada's Digital Content Advantage*
Discussion Questions:	• *What does creating Canada's digital content advantage meant to you?* • *How do you see digital content contributing to Canada's prosperity in the digital economy?* • *How can stakeholders encourage investment in development of innovative digital media?*
Recommendations:	**27. Commission an independent study on the feasibility and potential structures of alternative monetization models that will solve the problem of file-sharing while ensuring (a) rights holders are paid for distribution of content; (b) consumer needs currently fulfilled by unauthorized file-sharing are met; and (c) innovation in distribution of digital content is encouraged**

We have reached a critical impasse between distributors' desire to control channels for content distribution in the marketplace and the demand of many members of the public to access content outside of these channels.

The current situation – and it is one that has proved stable for more than a decade now – features both authorized distribution under the control or authority of a rights-holder and unauthorized distribution (at times dwarfing the volume of authorized channels), that thrives alongside authorized channels. Authorized and unauthorized distribution does not necessarily coincide with "monetized" and "pirated" distribution. Much authorized content distribution is not monetized, and is instead distributed alongside unauthorized content through file-sharing services or on the internet from sites not controlled by dominant content distributors. Other content is released under permissive licenses, such as Creative Commons licenses, which permit use and expect monetization only under certain conditions, such as commercial use. Clay Shirky observes that this "creative revolution" is "rooted in the opportunities afforded by connectivity."[120] Another noted factor is the lower barrier to entry for media companies and players. The massive fixed cost that had been required to join the newspaper or television space has been bulldozed by an endless number of small media impressions, from YouTube videos to Twitter tweets, and all the mid-sized entrepreneurial media companies in between that are running out of our neighbours' basements. These alternative business models and experimentation in distribution are to be encouraged as signs of healthy competition in the marketplace.

Experimentation and competition notwithstanding, however, the sad truth remains that consumers today still obtain much too much content through unauthorized channels, against the will of rights-holders, and without hope of compensating rights-holders for the value of that content.[121] Similarly, despite a decade of evidence that consumers want to use filesharing

[120] Clay Shirky, "Ambition: To Make the UK One of the World's Main Creative Capitals" (April, 2009), online: Digital Britain Reports <http://interactive.bis.gov.uk/digitalbritain/report/index.php?s=creative+revolution>.
[121] We set aside for the purposes of this discussion the availability of the private copying scheme to benefiting rights holders in the case of music downloading. Such benefits are not available to rights-holders of games, literary works or cinematographic works, and in any event offer user rights only to downloaders, not to those who "make available".

services to obtain content, the major content distributors have not stepped forward to license such services. While some have blamed this state of affairs on those doing the downloading – calling them "thieves" and describing the activity as "piracy"[122] – others have observed that those who engage in downloading also are more likely to acquire content through authorized channels.[123] Accordingly, downloaders wear multiple hats: "pirate" or "customer" – or "fan" – depending on the context.

Of greater interest is the policy response to this state of affairs. Ordinarily, responses to the disruptive impacts of new technologies take one of two forms: either market forces compel distributors to offer content to consumers on terms that leverage the benefits of the new technology, or, where the market fails to effectively leverage technology, policy-makers (or rights-holders through collectives) respond by transforming the exclusive rights involved into the equivalent of rights to remuneration. This second response entitles consumers to avail themselves of the content and technology involved in return for payment.

Canadian responses to the emergence of unauthorized file-sharing have taken neither of these forms. Currently, rights-holders in Canada and elsewhere have sought to sue individual defendants for engaging in unauthorized file-sharing.[124] It should be manifestly clear that this is not a legitimate policy outcome. Mass litigation, or the threat of litigation, is not a legitimate business model. Suing individuals misappropriates the resources of the tax-payer funded justice system and imposes costs, not born by the threatening party, out of proportion to the harm alleged. These concerns aside, suing file-sharers is a failed policy response to unauthorized file-sharing: it hasn't worked. Sharing unauthorized music files over the internet remains as popular as ever.

Marketplace responses in Canada have been limited. iTunes and other digital music stores are success stories in Canada, but do not compete effectively with the ease of use, comprehensive repertoire and low cost of peer-to-peer networks. Accordingly, these stores don't offer a solution to the problem of unauthorized filesharing: the practice is still widespread, and rights holders still are not being compensated.

Legislative responses to filesharing in Canada have proven even less imaginative. Bill C-32, *The Copyright Modernization Act*, does not propose to "solve" unauthorized filesharing. C-32 simply provides for more mechanisms by which rights holders might sue individual consumers – an endorsement of a failed strategy that will result in no authors receiving new payments for content shared without their permission.

This policy failure comes at a particularly crucial time for Canada's literary authors. The emergence of e-Readers that are acceptable to consumers, such as Chapters-Indigo's Kobo, has

---

[122] See *e.g.*, "What do the WIPO Treaties Say?" Canada_Version3.0, online: Facebook, <http://www.facebook.com/pages/Canada_Version30/138151172867661?v=wall#!/pages/Canada_Version30/138151172867661?v=wall> (Graham Henderson labeling copyright infringement "stealing").

[123] Brigitte Andersen and Marion Frenz, "The Impact of Music Downloads and P2P File-Sharing on the Purchase of Music: A Study for Industry Canada" (2007) at 3, online: Industry Canada <http://www.ic.gc.ca/eic/site/ippd-dppi.nsf/eng/h_ip01456.html>.

[124] *BMG Canada Inc.* v. *John Doe*, 2005 FCA 193, online: Federal Court of Appeal, <http://reports.fja.gc.ca/eng/2005/2005fca193/2005fca193.html>.

jump-started e-book sales. Pricing challenges and the prevalence of marketplace offerings dominated by digital locks strongly suggests that digital book publishing will also experience problems with unauthorized file-sharing. Book publishers receive the vast bulk of their writing income from royalties on sales. Without a mechanism for monetizing unauthorized distribution of e-books, literary authors will face increasing financial pressures.

It doesn't have to be this way in Canada. It shouldn't be this way.

Unauthorized filesharing shouldn't be illegal – it should be obsolete.

There are fresh ideas emerging in content distribution that bridge the gap between the content makers and their audiences. These ideas meet user expectations and allow creators to monetize the experience. Interestingly, the most promising of these ideas represent both sides of the traditional policy responses to technological challenges to copyright law: the marketplace response and the remunerative response.

Marketplace responses are beginning to emerge as companies like Spotify and We7.com enter the European marketplace. These services offer "cloud-based" experiences that provide users with affordable access to large repertoires of music. These services appear to be having an impact on unauthorized file-sharing. A survey of admitted users of file-sharing networks in the UK found that two in three reduced their number of downloads after using Spotify.[125] Bundling these services with internet service has also proven a convenient mechanism for obtaining and paying for the service. All parties to the transaction benefit. Why aren't these services available in Canada? Why aren't they even being talked about?

Legislative approaches have also been suggested. The Songwriters Association of Canada has proposed a working draft proposal regarding the online monetization of music which would establish a new right: "The Right to Remuneration for Music File Sharing."[126] This approach calls for a voluntary licensing scheme whereby rights holders agree to permit private non-commercial "sharing" of content, regardless of the mechanism, in return for payment of a sum determined by a neutral decision maker. Consumers would only pay for the content if they choose to. Again, a simple and elegant solution that has enjoyed no traction in Canada.

Barriers to solutions – both marketplace and legislative – include the continuing high cost of bandwidth in Canada. Rob Hall, President of Zip.ca, a movie rental service, has told the CRTC that he would like to get in the online movie distribution business, but the cost of bandwidth is a barrier:

[125] Daniel Bennett, "Spotify reduces illegal downloading in UK" (6 Nov 2009), online: The Gadget Website <http://www.t3.com/news/spotify-reduces-illegal-downloading-in-uk?=42021>.
[126] Songwriters Association of Canada, "Our Proposal: Detailed" (March 2009), online: Songwriters Association of Canada <http://www.songwriters.ca/proposaldetailed.aspx>.

> Right now it costs more for us to download the video than to ship it by mail....In the U.S. this wouldn't be true. We can buy bandwidth much cheaper in the U.S. than we can in Canada. However, we have always decided to keep our video servers in Canada.[127]

The Government of Canada, as a part of the Digital Agenda, has an important role to play in encouraging dialogue between all stakeholders. CIPPIC believes the government can start this dialogue by commissioning an independent study of the feasibility of marketplace and collective approaches to solving the problem of unauthorized filesharing. The objective of this study should be to identify policy options that have the complementary objectives of:

(a) creating a structure by which rights-holders will be paid for distribution of content;
(b) meeting consumer needs currently fulfilled by unauthorized file-sharing; and
(c) encouraging innovation in the distribution of digital content.

The study should have the power to gather evidence, consult widely and conduct original research. It should be independent of both political and marketplace influence. The Gowers Commission in the United Kingdom provides a model upon which the government might base such a commission.[128]

IX. Open Data

Theme:	*Growing the Information and Communications Technology Industry*
Discussion Questions:	• *Do current investments in R&D effectively lead to innovation, products and services?* • *What is needed to innovate the ICT industry?*
Recommendations:	**28. Adopt open data policies;**

Canadian researchers, businesses, and citizens need an open data portal where they can access public sector data in open formats. This will help bring Canadians further government transparency and social value. It will help Canadians exercise their fundamental democratic right to participate in government by allowing them to make their own decisions, and help the government make decisions, on policies driven by public sector input. It will help promote new and innovative industries in commercial research, and in useful consumer software built around the data. It will help increase productivity across Canadian market sectors.

In the U.S., as part of an open data initiative, every single federal department was required to publish a road-map for making operations and data more transparent.[129] A U.S. website dedicated to openly providing government data, www.data.gov, now distributes over 270 000 government datasets.[130] The U.K. open data portal, data.gov.uk, distributes thousands of datasets

---

[127] Submissions of Rob Hall, Transcript of Proceedings Before The Canadian Radio-Television and Telecommunications Commission, CRTC Telecom 2009-19, Review of the Internet traffic management practices of Internet service providers, (July 7, 2009), online: CRTC <http://www.crtc.gc.ca/eng/transcripts/2009/tt0707.htm>.
[128] See "Gowers Review of Intellectual Property" (December 2006), online: The National Archives <http://webarchive.nationalarchives.gov.uk/+/http://www.hm-treasury.gov.uk/gowers_review_index.htm>.
[129] See U.S., White House Open Government Initiative, "Around the Government" (2010), <http://www.whitehouse.gov/open/around>.
130 U.S., Data.gov, "Data.gov Catalogs", <http://www.data.gov/catalog>.

from across different government departments.[131] These diverse datasets range from water quality assessments to population densities to regional health insurance estimates. Hundreds of research and consumer applications are already making use of this data.[132]

Canada, with no federal open data portal and no road-map for making government data openly available, is at serious risk of falling behind in research and the development of secondary markets around public sector data, depriving Canadians of the immense benefits that a vibrant application and research community built around open data can offer.

A. Government Transparency & Social value

Opening access to public sector data will allow citizens to better engage with the government and its policies. By granting citizens access to the data on which the government bases its decisions, citizens can analyze the data in new ways and provide feedback and creative ideas. In the U.K., for example, any interested citizen can view detailed and customized analytics on government expenditures.[133] In the U.S., any citizen can use an application to visualize and analyze public health data.[134]

Other applications provide helpful and practical tools for citizens. Canadians have already built innovative applications utilizing city data released by several municipalities. Applications built on the City of Vancouver's open data portal allow citizens to track their garbage and recycling schedules, find parking spots, and locate nearby water fountains.[135]

B. Private and Public Sector Research

The release of government data could also realize substantial economic benefits in the Canadian research sector. It could enable commercial researchers to generate new markets by adding value to data through the provision of advanced searching, data visualization, data syndication, and data analysis and correction.

Additionally, private and public research initiatives would be able to use the data to help stimulate economic growth and increase economic productivity. A report on open data by the Australian government estimates that the availability and use of government spatial data alone would increase productivity by billions of dollars, in industries such as agriculture, fisheries, and resource exploration – industries also of fundamental importance to Canada.[136] For example, increased access to spatial data in agriculture can improve yield monitoring, soil condition

---

131 U.K., Data.gov.uk, "List All Datasets", <http://data.gov.uk/data/all> (accessed 8 July 2010).

132 See e.g. U.K., Data.gov.uk, "Apps List", <http://data.gov.uk/apps/list> (accessed 8 July 2010) [*U.K. Apps*]; Apps for Democracy, "Application Directory", <http://www.appsfordemocracy.org/> (accessed 8 July 2010) [*U.S. Apps*].

133 RA.Pid Spend Analytics application, <http://data.gov.uk/apps/rapid-spend-anaytics>.

134 Data visualization of the US Department of Health and Human Services application, <http://health.jameyer.com/>.

135 Vantrash application, <http://vantrash.ca/>; Vancouver Parking 2010 application, <http://www.vanpark2010.ca/>; Water! application, <http://water.tylorsherman.com/>.

136 See Australia, Department of Finance and Deregulation, "Engage: Getting on with Government 2.0" (2009), at 43, online: Australian Government: Department of Finance and Deregulation <http://www.finance.gov.au/publications/gov20taskforcereport/doc/Government20TaskforceReport.pdf> [*Engage Report*].

mapping, pest and disease control, and farm planning.[137] In the fishing industry, access to spatial data can improve habitat monitoring, safe navigation, weather forecasting, and aquaculture planning.[138]

C. Consumer applications

The availability of government data could also open up new possibilities for innovation in the consumer software industry. The U.S. and U.K. open data initiatives demonstrate that open government data can be used to create innovative software tools. First-generation applications allow users to create customized city tours, find care homes, and locate the nearest banks and gas stations.[139] In the future, business models are likely to develop around monetizing similar and even more intricate applications..

D. Reduction of Taxpayer Costs

The complex research of today and tomorrow often requires collaboration between companies and with the public sector. Currently, companies and researchers must purchase government datasets on a cost recovery basis, usually after navigating complex licensing agreements. Once purchased, these licensing agreements can continue to burden data sharing with other companies and organizations involved in a particular research effort.

The government costs in administering these licensing regimes, combined with the costs to researchers and businesses, results in a net loss to Canadians. These datasets are already paid for by Canadian taxpayers. They should not need to be purchased again by Canadian citizens, and Canadians taxpayers should not be burdened with the costs of managing these second sales. To enable Canada to continue as a research, economic leader in the digital economy, Canada must ensure that data paid for by taxpayers is made available to all taxpayers.

E. Drawbacks?

Moreover, there appears to be no economic downside to opening Canadian government data. There is generally no marketplace competition for the data collected by the government, so it would not have a detrimental impact on existing businesses. Moreover, these datasets are, by nature, "non-rival"; unlike physical goods, sharing these datasets will not decrease their value.[140] On the contrary, sharing can increase the value of the data when services and new ways of analyzing data are built on top of it.

Overall, the only cogent downside to data openness is the privacy issues that it can raise. However, many datasets can be released in their entirety without raising the possibility of disclosing the personal information of Canadians. For other datasets, the possibility of disclosing personal information can be mitigated by careful consideration of the granularity of the data released, as well as, where necessary, the imposition of licensing restrictions on the way that commercial advertisers are permitted to combine the data with other sources of information.

---

137 See ACIL Tasman, "The Value of Spatial Information" (2008), <http://www.crcsi.com.au/UPLOADS/PUBLICATIONS/PUBLICATION_324.pdf> at 28-33.

138 *Ibid. at* 41.

139 See *U.K. Apps*, *supra* note 4; *U.S. Apps*, *supra* note 4.

140 See *Engage Report*, *supra* note 5.

F. A Policy of Openness

Governments within Canada and around the world are developing policies of data openness to improve government transparency and engage their citizens. This movement is consistent with maximizing taxpayer value, both social and economic. The federal government needs to release public sector data under public domain or unrestricted licenses, in open formats. Where there are no significant security or privacy concerns, a practice of data openness needs to be the default rule, rather than the exception.

X. Broadband Access and Infrastructure

Theme:	*Growing the Information and Communications Technology Industry*
Discussion Questions:	• *Do current investments in R&D effectively lead to innovation, products and services?* • *What is needed to innovate the ICT industry?*
Recommendations:	**29. Ensure open access and structural/functional separation;** **30. Task an independent body to gather data on average traffic speeds;** **31. The government should consider public investments in urban and rural investments;** **32. Declare affordable access to high speed broadband to be a fundamental right;** **33. Set ambitious, short term targets for universal or near universal broadband access at affordable rates;** **34. Make provisions to provide Internet access subsidies to lower income Canadian households;** **35. Create funding for community initiatives to provide free WiFi hotspots;** **36. Ensure principles of net neutrality remain in place;**

- The government should encourage and fund community initiatives to provide free internet access in densely populated areas.
- We support the recommendation that legislation and regulation to protect network neutrality in Canada should be continually reviewed and adapted to safeguard innovation and the interests of Canadians in general.[141]

Digital technology is becoming more and more an essential part of our modern lives. Broadband access to internet improves the lives of individuals, by facilitating access to information, increasing business opportunities, improving digital skills and allowing citizens' involvement in the public life of their community and beyond. Basic everyday activities, such as banking, education, social services and job searches, are currently being offered predominantly online with many other services soon being offered online.

Technology is evolving at a fast pace and for a successful digital Canadian economy, the government should anticipate, develop and implement strategies to face and support any future technological advances, not just comply with the present. As stated by Tony Clement, the

[141] *Ibid.*

Minister of Industry, Canada is falling behind other countries in adhering to new technologies,[142] this is impacting on our economy, innovation and prosperity in general, as well as on the ability of our citizens to participate in the global digital economy.

Universal access to broadband should be our government's highest priority when planning for a digital future in Canada. "Universal" should be defined as 100% of citizens and nothing less, as recommended by the Standing Senate Committee on Transport and Communications in its *Plan for a Digital Canada*.[143] High speed access to the internet and other digital services should also be equitable, reliable and affordable.

A. How to regain Canada's lost digital advantage?

Countries ranking highest in broadband penetration per 100 inhabitants, such as Sweden and Denmark, also demonstrate high degrees of internet speed and low prices. Once a leader in Internet access, more recent studies rank Canada as low as 19th overall among OECD countries, mostly due to weak performance in price and speed, as well as 3G penetration.[144]
Canada must take steps to regain its early success in the global digital landscape. This can be done in a number of ways. A study conducted for the FCC concluded that in order to ensure infrastructure investment and reasonable pricing, open access and functional or structural separation are required to ensure a sufficiently competitive environment.[145] The government should particularly ensure competitor resellers are given access to next generation high speed services. Without competition on such services, there is no impetus on incumbents to invest in infrastructure and to provide it at affordable rates.

In addition, the government or the CRTC should be funding and providing the impetus for rigorous testing of average speeds, latency and jitter. It is not sufficient to have high advertised speeds. These speeds must be reflected by sufficient investment in network infrastructure, yet there is little data available on average speeds across different service providers. By better informing consumers on average speeds in addition to advertised speeds, the government can make infrastructure investment, not just modem speeds, a competitive issue and stimulate greater investment.

Section Recommendation:

- Ensure open access and structural or functional separation to instil competition in investment and price;
- Gather and publish traffic measurements on average speeds to stimulate competition on internal network investment within the network itself;

---

[142] Matt Harley, "Canada falling behind on tech front" *Financial Post* (11 May 2010), online: Canada.com <http://www.canada.com/Canada+falling+behind+tech+front/3013210/story.html>.
[143] Canada. The Standing Senate Committee on Transport and Communications, "Plan for a Digital Canada" recommendation 5, online: Plan for a Digital Canada <http://www.planpouruncanadanumerique.com/index.php?option=com_content&view=article&id=4&Itemid=13&lang=en>.
[144] Berkman Center for Internet & Society at Harvard University, Next Generation Connectivity: A Review of Broadband Internet Transitions and Policy from Around the World, (Final Report, February 2010), "Table 3.8. Country ranks based on weighted average aggregates," at 81, online: Berkman Center for Internet & Society <http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Berkman_Center_Broadband_Final_Report_15Feb2010.pdf>.
[145] *Ibid.*

- The government should consider investing in urban as well as rural broadband infrastructure to encourage higher speed broadband development.

B. Broadband in Rural Areas

Many Canadians living in rural or less populated areas do not enjoy access to broadband internet at acceptable speeds. This digital divide between the rural and urban areas makes it hard for the rural economy to prosper.

Broadband access would allow communities to connect globally, to attract new firms and investments, as well as to compete with other communities. It would also spur innovation and revitalize rural communities generally left out of the digital revolution.

Bringing high speed internet to remote rural areas is a challenge that has to be overcome in order to attain the goal of having a truly universal digital economy. The vast and varied geography of Canada is one of the barriers to accomplishing this goal of providing same internet advantages in the rural areas as available in the urban centres. The government should focus on providing a reliable, affordable and effective access to Internet in these areas so citizens living away from densely populated areas can benefit from and participate in Canada's digital society.

Rural broadband presents another example where there is a pressing public policy objective that the market is not likely to solve on its own. There is little to no competition over broadband provision to rural areas because of the steep costs and little hope for large returns.[146] It is nonetheless a pressing policy objective and should be made a priority for any government taking seriously its intention of crafting a competitive global digital economy.

As there is unlikely to be a competitive solution to this situation, one solution may be to solve the problem with public investment. Other jurisdictions have provided heavy public investment and were successful in addressing the digital divide in that manner.[147] In addition, CIPPIC endorses the recommendation of The Standing Senate Committee on Transport and Communications (recommendation 15) calling for 2% of revenues from spectrum license holders to be spent on building an infrastructure to deliver broadband in areas where it is unavailable at the moment.[148] CIPPIC believes government investment has a significant role to play in ensuring Canada's digital infrastructure reaches those Canadians not fortunate enough to live in areas where high-level private industry investment can be profitable.

<u>Section Recommendations</u>:

- Invest public funds in rural broadband infrastructure to ensure rural areas receive access to high speed broadband services and are able to participate in the digital economy;

---

[146] Iain Marlow and Jacquie McNish, "Canada's digital divide" *The Globe and Mail,* (2 April 2010), online: The Globe and Mail: <http://www.theglobeandmail.com/report-on-business/canadas-digital-divide/article1521631/>.

[147] Australia, for example, has pledged A$43 billion in a joint public/private venture to increase broadband capacity everywhere, including rural areas. See below for more details.

[148] Canada. The Standing Senate Committee on Transport and Communications, "Plan for a Digital Canada", Recommendation 15, online: Plan for a Digital Canada <http://www.planpouruncanadanumerique.com/index.php?option=com_content&view=article&id=4&Itemid=13&lang=en>.

- Invest in digital skills education programs to compliment rural investment so as to maximize benefits and reach of investment in rural infrastructure.

C. Internet as a fundamental right

The government should join others in declaring broadband internet access a fundamental right for all Canadians. Such access should be at minimum 2Mbps, but the government should set more ambitious targets for universal access if it wishes to regain Canada's digital supremacy.

In 2009 Britain, for example, set a target of 2 Mbs for all British citizens to be attained by 2012.[149] Australia aims to offer 100 Mbs to 90% of its denizens by 2017,[150] a plan that would cost A$43 billion and would be a joint venture between the government and the private industry.

Japan has some of the fastest and most affordable connections in the world. Providing broadband access in the rural areas of Japan, has improved the job opportunities for those citizens living outside major cities, as well as encouraged migration from the city to the countryside.[151] The Japanese government subsidized the installation of a fast fibre-based FTTH 1Gb/second (fibre-to-the-home) network and the service is available at a very reasonable price per speed.

In 2009 in the US, Minnesota State has introduced a bill which calls for 1 Gbs of symmetric bandwidth to *all* Minnesotans by 2015. Similar initiatives have been noted in California.

Affordability is an important element to be considered when setting targets for a truly universal access to broadband. It is difficult and hardly justifiable for a low-income family to subscribe to a high-priced broadband service. Complaints about quality of service and billing practices can also lead existing subscribers to discontinue their internet access services. These considerations further the digital divide in our society, where access to broadband is a luxury only some can afford to use and subscribe to at home.

Section Recommendations:

- Declare Internet access as a fundamental right;
- Set ambitious, short term targets for universal or near universal broadband access at affordable rates;
- Make provisions to subsidize access for those who are below certain annual income levels;

D. Hotspots in densely populated areas

Access to internet services is a basic essential service and affordability is an important consideration. Even when internet is available locally, a large number of Canadians do not have access to it due to expensive monthly subscriptions. One practical solution to such problems would be the availability of free WiFi hotspots in communities, so citizens have access to information, communications (such as e-mail, social networking), e-commerce (for a larger more

[149] Digital Britain, (Final Report, June 2009), online: Department of Business Innovation & Skills <http://berr.gov.uk/assets/biscore/corporate/docs/d/10-810-digital-economy-bill-impact-assessments.pdf>.
[150] *Ibid*. at 81.
[151] Michael Fitzpatrick, "Broadband goes big in Japan" *BBC News* (26 May 2009), online: BBC <http://news.bbc.co.uk/2/hi/technology/8068560.stm>.

competitive market), and other essential day to day services that are and will continue to be offered predominantly online.

Community innovation can spur from the people's desire to access and enjoy the benefits of the internet everywhere. Wireless technologies are an inexpensive way to provide internet to citizens. A volunteer group in Montreal installed and operated a network with 150 WiFi internet 'hotspots' covering the downtown Montreal Ile, providing free internet access to more than 50,000 users.[152] Similarly in Minneapolis, MN the city has installed 117 hot spots for citizens and visitors to access the internet for free. Initiatives like this cut across priority areas, such as infrastructure and content, and should be encouraged and supported in all communities to further the main goal of creating a digital future in Canada.

Section Recommendation:

- The government should encourage and fund community initiatives to provide free internet access in densely populated areas.

E. Net Neutrality

For innovation and economy to prosper in our society, net neutrality plays an essential part. Everyone should be able to transmit and receive data and information on the internet in a non-discriminatory way. Cable companies cannot be allowed to filter, throttle or shape the traffic over their networks, as this practices "run counter to the principles of network neutrality."[153] ISPs argue though that prohibiting any kind of bit prioritization will lead to an increase in service provider costs, as networks would have to be expanded to alleviate congestions.

Section Recommendation:

- We support the recommendation that legislation and regulation to protect network neutrality in Canada should be continually reviewed and adapted to safeguard innovation and the interests of Canadians in general.[154]

Conclusion

With technology evolving at a fast pace and the increasing need of citizens to access broadband internet, the government cannot be content with bringing Canada into the digital present, but should plan strategies to anticipate any future developments and advances in the digital world. High speed access to the internet and other digital services has to be ubiquitous, equitable, reliable and most of all affordable for a successful and prosperous digital economy in Canada.

[152] Andrew Clement, Consultation, Telecom Notice of Consultation CRTC 2010-43, (26 April 2010), at 6, online: CRTC <http://www.crtc.gc.ca/public/partvii/2010/8663/c12_201000653/1387417.PDF>.
[153] Andrew Clement and Karen Louise Smith, coordinators, "Interim Consensus Submission to the federal government consultation on a Digital Economy Strategy for Canada" (4 July 2010), online: <http://ipsi2010.pbworks.com/>.
[154] *Ibid.*