Samuelson-Glushko Canadian Internet Policy & 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

Assemblée nationale du Québec
LA COMMISSION DES INSTITUTIONS

Technologies et vie privée à l'heure des choix de société

Privacy & the Right to Information in a Rapidly Evolving Technological Landscape

WRITTEN SUBMISSIONS OF THE SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY & PUBLIC INTEREST CLINIC (CIPPIC)

March 30, 2013

Submission By

Tamir Israel, Staff Lawyer
Alexander Cooke, Law Foundation of Ontario Public Interest Fellow
Afsoun Amirsolaimanimazandarani, CIPPIC Student Intern

TABLE OF CONTENTS

Introduction

1. The Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC) is pleased for this opportunity to present its comments on this important consultation. We note at the outset that Quebec's privacy protection and open government regimes have many strong points in their favour. However, as we expand upon below, more must be done if these important rights are to be respected in full in a technologically advanced and interconnected society.

CIPPIC

2. CIPPIC is a public interest legal clinic based at the University of Ottawa's Centre for Law, Technology & Society. CIPPIC's advocacy covers diverse technology-related issues, several of which relate to the right to access information and the protection of privacy in various and wide-ranging contexts. Pursuit of its public interest mandate includes expert testimony before parliamentary committees, interventions in Canada's judicial system, appearances and submissions to various tribunals such as the Office of the Privacy Commissioner of Canada, and participation in international Internet governance fora. In addition, CIPPIC advises clients (organizational and otherwise) on matters with a public interest dimension and provides public education resources on various legal issues.

3. Privacy and data protection have been central to CIPPIC's mandate since its inception. CIPPIC's institutional experience includes active participation in the development and ongoing modification of the Personal Information Protection and Electronic Documents Act (PIPEDA), our federal data protection statute.[1] In addition, CIPPIC has filed over 20 privacy complaints under PIPEDA on data protection matters such as the privacy practices of social networking sites,[2] the use of mid-network collection of Internet Service Provider customer's data for the purpose of traffic management using

[1] For a recent example, see: http://cippic.ca/Privacy_and_Emerging_Technologies
[2] http://cippic.ca/Facebook

Deep Packet Inspection network equipment,[3] the implications of online data breaches of sensitive data,[4] the cross-jurisdictional data collection practices of US-based websites and web-based services,[5] and the potential privacy implications of the Google/Double-Click merger,[6] to name a few. CIPPIC has additionally participated in the review of international data protection regimes, including the Council of Europe's Convention 108,[7] and the OECD's Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,[8] as well as in the early development of the APEC Cross Border Privacy Rules framework.[9]

4. Information rights have similarly played a prominent role in CIPPIC's activities. CIPPIC has had frequent recourse to the use of various federal and provincial freedom of information regimes as part of its broader advocacy mandate. As such, we have on the ground experience on the challenges and limitations of the utility of such legal regimes. In addition, CIPPIC has been an active participant in broader open governance debates,[10] and has produced several reports on open data-related matters.[11] Finally, as one of three affiliate organizations operating Creative Commons Canada, CIPPIC recognizes the importance of simplifying complex legal language and facilitating greater fluidity for information exchange once data sets are available.[12]

I. Technology & Privacy: Keeping up with the Times

(a) The Hope of Transparency: Trust without Substance?

Recommendation 1: *The Commission recommends that the legislator oblige public bodies and businesses to adopt simplified confidentiality policies*

[3] http://cippic.ca/DPI
[4] http://cippic.ca/Data_Breach_Notification
[5] http://cippic.ca/outsourcing and http://cippic.ca/SWIFT
[6] http://cippic.ca/GoogleDoubleClick
[7] http://cippic.ca/ETS_108
[8] http://cippic.ca/OECD_Guidelines
[9] http://cippic.ca/APEC_CBPR
[10] http://cippic.ca/OIC_consultation
[11] http://cippic.ca/open_governance
[12] http://creativecommons.ca/about

presenting, in clear and comprehensible terms, an overview of their undertakings for the protection of personal information.

Recommendation 2: *The Commission recommends that the legislator impose on public bodies and businesses the use of protection pictograms informing individuals of their undertakings for protection of personal information.*

5. The increasing extent to which privacy is becoming commoditized and the growing scope and complexity of data protection practices undertaken by companies are well documented.[13] The length of privacy policies have grown apace,[14] making it difficult for individuals to understand precisely how their information will be collected, used, disclosed and retained. Exacerbating the length and often convoluted nature of privacy policies is their ubiquity – one study estimated that if all U.S.-based Internet users were to annually read the privacy policy for each site they encounter once annually, the opportunity cost value of time spent reading would be $781 billion.[15] In CIPPIC's experience, privacy policy drafting processes are often less an attempt to explain privacy practices to customers, and more an exercise in liability limitation. This leads not only to often legalistic language, but also to broad clauses capable of covering a range of practices as well as the ubiquitous right to overhaul existing practices at will.[16]

6. Adopting a principle of simple language, and the inclusion of an overview is a positive step towards improving customer understanding of how their information will be collected, used and disclosed. Some form of standardized graphics can build on this

[13] See, for example, the Wall Street Journal's ongoing "What They Know" investigative series: Wall Street Journal, "What They Know", <http://online.wsj.com/public/page/what-they-know-digital-privacy.html>.
[14] N. Bilton, "Price of Facebook Privacy? Start Clicking", May 12, 2010, New York Times, <http://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html>.
[15] A.M. McDonald & L.F. Cranor, "The Cost of Reading Privacy Policies", (2008) *I/S: A Journal of Law and Policy for the Information Society*, 2008 Privacy Year in Review, <http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>. This amount would have eclipsed the cost of high speed Internet access, as well as the $260 billion 2007 U.S. online sales market (*Ibid.*).
[16] I. Paul, "Instagram Updates Privacy Policy, Inspiring Backlash", December 18, 2012, PC World, <http://www.pcworld.com/article/2021285/instagram-updates-privacy-policy-inspiring-backlash.html>. Also see: T. Israel, "CIPPIC Comments on Office of the Privacy Commissioner of Canada's Draft Report on the 2010 OPC Consultations on Online Tracking, Profiling and Cloud Computing", December 20, 2010, <http://www.cippic.ca/sites/default/files/20101220-CIPPIC-Comments-OPCDRAFTREPORT.pdf>, p. 6.

transparency by helping individuals understand, with minimal time investment, long and often convoluted explanations. However, it must be recognized that privacy practices are inherently complex and may not be readily reduced into brief overviews or images. As pointed out by noted Carnegie Mellon researcher Alessandro Acquisti: "…transparency and control are empty words that are used to push responsibility to the user for problems that are being created by others."[17]

7. The use of privacy symbols as a means of conveying privacy practices has proven problematic in the past. For example, the Digital Advertising Alliance developed an icon to better inform individuals of data protection practices arising from online tracking for the purpose of providing targeted advertising.[18] Few participants understood that the icon indicated the advertisement accompanying it was targeted to their interests and *none* understood it indicated their online browsing activities were being tracked.[19]

8. Other graphic privacy indicators such as privacy seals were intended to convey a site's compliance with a basic and established set of privacy practices. However, research indicates that the presence of a privacy seal, while perhaps lowering privacy *concerns*, in many cases will provide little if any verifiable differences to privacy practices:

> Thus, privacy seals that are supposed to function as privacy and data protection indicators often become misleading beacons, shielding low privacy standards.[20]

---

[17] S. Sengupta, :Letting Down Our Guard with Web Privacy", March 30, 2013, New York Times, <http://www.nytimes.com/2013/03/31/technology/web-privacy-and-how-consumers-let-down-their-guard.html>; L. Brandimarte, A. Acquisti & G. Loewenstein, "Misplaced Confidences: Privacy and the Control Paradox", *WEIS'10*, August 2012, *Social Psychological and Personality Science*, available at: <http://www.futureofprivacy.org/wp-content/uploads/2010/07/Misplaced-Confidences-acquisti-FPF.pdf>.

[18] B. Ur, P.G. Leon, L.F. Cranor, R. Shary & Y. Wang, "Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising", CMU-CyLab-12-007, April 2, 2012 (revised July 13, 2012), <https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12007.pdf>, p. 5.

[19] B. Ur, P.G. Leon, L.F. Cranor, R. Shary & Y. Wang, "Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising", CMU-CyLab-12-007, April 2, 2012 (revised July 13, 2012), <https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12007.pdf>, p. 5.

[20] R. Rodriguez, D. Wright & K. Wadhwa, "Developing a Privacy Seal Scheme (That Works)", (2013) *International Data Privacy Law*, <http://idpl.oxfordjournals.org/content/early/2013/01/31/idpl.ips037.full.pdf+html> , p. 7.

Indeed, some surveys of sites using the two most established privacy seals (TRUSTe and BBBOnLine) concluded that these sites were *more* likely to infringe on user privacy than uncertified sites.[21]

9. Additionally, it is important to note that pictogram schemes have been mostly successful when appended in order to *waive* rights, not to *take* them away. Creative Commons, for example, provides a broadly used and highly sophisticated set of pictograms which permit individuals to *waive* rights in works in order to facilitate broader dissemination of those works. Privacy pictograms, however, would operate as a form of waiver *imposed* on an individual so that the service employing them can make free use of the employer's personal information without impediment. Further, where it is a simple manner to standardize a *grant* of rights, since the complexity and variety of use will ultimately rest with the grantee, the same cannot be said for an attempt to capture complex and varying practices on the side of the *grantor(s)*. The success of any privacy pictogram system will depend on accounting for the important differences in incentives that accompany these two very different contexts.

10. This is not to say that graphic icons cannot play a role in improving people's understanding of how their personal data is being used. Standardization of field headings, for example, will help individuals become accustomed to looking in the same place for details on comparable privacy practices, for example. It is additionally clear that an effective privacy pictogram system must be accompanied by consistent and proactive regulatory monitoring for compliance and robust enforcement. Finally, great care must be taken not to attempt to capture complex data protection practices in simple graphics as this may well turn into a process of trust without substance.

> **Suggestion 1:** Caution should be taken in the adoption of any image-based or otherwise overly simplified privacy communication mechanisms or obligatgions.

[21] R. Rodriguez, D. Wright & K. Wadhwa, "Developing a Privacy Seal Scheme (That Works)", (2013) *International Data Privacy Law*, <http://idpl.oxfordjournals.org/content/early/2013/01/31/idpl.ips037.full.pdf+html> , p. 8.

Recommendation 3: *The Commission recommends that the legislator oblige public bodies and businesses to report the presence of mechanisms likely to identify or locate a natural person during use of their products.*

Recommendation 4: *The Commission reminds public bodies and businesses to integrate the principles of protection of personal information when they design their goods and services and to apply them throughout the life cycle of this information.*

11. Singling out location services is useful, but ultimately a more flexible approach would be desirable. The challenges that location-tracking services pose to privacy are not specific to these types of technologies, and should be addressed in a more principled manner that will carry across other problematic current and future technologies.

12. The challenges inherent in location technologies are two-fold. First, location tracking may not always clearly and unequivocally be traced to an 'identifiable natural person', potentially taking the collection (but not use) of such information outside the scope of data protection laws. This is because it is frequent, these days, to track 'individuals' by device, browser-based cookie, or other comparable mechanism as opposed to by name alone. While location information is highly capable of revealing natural identity,[22] some may rely on any existing ambiguity on this point to ignore privacy protections on the premise that the information is not 'about an identifiable individual'.

13. This issue, however, is by no means unique to location tracking. The same arguments are occasionally advanced with respect to other types of tracking, notably tracking of online browsing or similar activity, which is often traceable back to an IP address, or unique cookie-based identifier. This is because online tracking mechanisms, and particularly those that are commercially driven, can often achieve their purposes (targeted tracking, customer profiling, price discrimination, etc.) without ever discovering the identity of the natural person.

[22] One recent comprehensive study of human mobility data found that of 1.5 million data sets where location was collected on an hourly basis over time, four spatial/temporal points were sufficient to identify 95% of individuals: Y-A de Montjoye, C.A. Hidalgo, M. Verleysen & V.D. Blondel, "Unique in the Crowd: The Privacy Bounds of Human Mobility", (2013) 3 *Scientific Reports* 1376, <http://www.nature.com/srep/2013/130325/srep01376/pdf/srep01376.pdf>.

14. A more principled solution to this issue will provide a comprehensive response to what is an endemic and problematic feature of technological tracking capacity. In addition, this type of information collection should benefit from the full panoply of privacy protections available, not merely the enhanced reporting obligations suggested in Recommendation 3. Instead of a general obligation to inform individuals of mechanisms intended to attempt to locate or identify natural individuals, we suggest applying the general protections found in *An Act Respecting the Protection of Personal Information in the Private Sector*,[23] to ensure it applies to the collection, use, disclosure and retention of any information likely to be linked to an identifiable individual or to a specific computer or other comparable device.[24]

> **Suggestion 2:** Apply Quebec's privacy protections to the collection, use, disclosure and retention of any data likely to be linked to any identifiable individual, computer or other comparable device.

15. The second problematic feature that is inherent in the tracking of location information is its significant capacity to reveal previously undisclosed, yet highly sensitive information about an individual's personal life, aspirations, opinions, beliefs, medical conditions financial stability or general activities. This is problematic not only because of the sensitive nature of the information revealed, but also because of the manner in which it is revealed – often by piecing together multiple, individually innocuous data points over time, as ably explained by a D.C. Circuit Court in the context of police surveillance:

> Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can

[23] R.S.Q. c P-39.1, <http://www.canlii.org/en/qc/laws/stat/rsq-c-p-39.1/latest/rsq-c-p-39.1.html>.
[24] A comparable definition has been suggested by the U.S. Federal Trade Commission: FTC, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers", March 2012, <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>, p. 15-18: The FTC framework applies to "all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device."

> reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts.[25]

On this basis, enhanced notification for location tracking mechanisms is justified but not, in our view, sufficient. The digital environment not only dramatically expands the scope of sensitive information capable of being collected on individuals, but also, in many instances, allows for similar 'piecemeal' profiling in which constituent elements may not be 'sensitive', but the whole provides a level of insight into individuals' lives that is sensitive and highly invasive.

16. As such, we suggest that a number of measures be adopted to ensure that Canadians receive the type of information they deserve *whenever* the privacy of their sensitive information is put at risk. First, we suggest the enhanced notification requirement suggested in Recommendation 3 be applied to *all* instances in which sensitive information is being collected.

17. Additionally, given the increasingly sophisticated manner in which information is being collected, interconnected, analyzed, and shared, CIPPIC recommends imposing clearer obligations on organizations when seeking consent for such practices. Specifically, CIPPIC suggests the adoption of comparable language to that proposed in Clause 5 of Bill C-12, which seeks to amend PIPEDA:

> 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.[26]

---

[25] *U.S. v. Maynard*, 614 F.3d 544, (U.S. D.C. Circ., 2010), p. 562, affirmed in part in *U.S. v. Jones*, 565 U.S. __, (2012).

[26] Bill C-12, Safeguarding Canadians' Personal Information Act, September 29, 2011, First Reading, 1sst Session, Forty-first Parliament, 60 Elizabeth II, 2011, <http://www.parl.gc.ca/content/hoc/Bills/411/Government/C-12/C-12_1/C-12_1.PDF>.

This will obligate organizations to ensure that they take proper measures to fully inform Canadians as to how their information will be collected, used and disclosed before their consent can be relied upon.

18. Additionally, we note that Recommendation 4 suggests the adoption of a core element of privacy by design: the incorporation of privacy principles into all elements of the product design process. We note, however, that this is not enough in and of itself. An explicit obligation to *minimize* data collection, use and disclosure at *all* levels of the data handling process is necessary in an era where so much information is so easily available. Data minimization has been long been recognized as a foundational principle in data protection[27] and, more recently, was recently adopted by the United States administration in its Consumer Data Privacy Bill of Rights.[28]

19. Finally, we note that Recommendation 4 ignores what is the most important aspect of the privacy by design suite of obligations: privacy by default.[29] The explicit adoption of this principle as an independent obligation is necessary to ensuring privacy in a rapidly evolving and technologically advanced age. Obligating privacy by default as an overriding principle of service design will ensure individuals are aware that their information is being processed, and reduces the burden and often significant effort individuals must undergo when attempting to navigate often complex and frequently changing privacy settings in digital services.

> **Suggestion 3:** Apply the obligation in Recommendation 3 for enhanced notification to ensure it applies to any and all mechanisms that seek to collect, use or disclose sensitive personal information.

---

[27] OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>, section 7.

[28] White House, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy", February 2012, <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>, Principle 6.

[29] A. Cavoukian, Information & Privacy Commissioner of Ontario, "Privacy by Design: The 7 Foundational Principles", Last Revised January 2001, <http://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf>.

Suggestion 4: Ensure that organizations seeking to collect, use or disclose an individual's personal information on the basis of her consent only do so if it is reasonable to expect the individual understands the nature, purpose, impact and consequences of consenting.

Suggestion 5: Impose onto organizations the obligation to minimize data collection, use and disclosure at all stages of the data handling process.

Suggestion 6: Adopt the obligation to respect privacy by design as an overriding obligation in service design, at least with respect to sensitive information.

(b) Digital natives

Recommendation 5: *The Commission recommends that the school system develop curricula at the elementary and secondary level to educate youth about IT and Web 2.0 issues.*

Recommendation 6: *The Commission invites the legislator to consider the appropriateness of amending consumer protection or personal information legislation, particularly to prohibit profiling of minors in electronic environments.*

20. With respect to recommendation 5, the integration of educational programs in children's curriculum is an important step. We live in an era where individuals are connected to the internet at a young age and it is therefore essential to begin educating them about the implications as well as the risks involved in engaging in online activities. Providing children with digital skills can also provide for a safer online experience, as youths will be better placed to identify attempts at fraud and other potential online hazards.

21. With regards to recommendation 6, CIPPIC is in accordance with the proposition that the protection of children's online privacy is a concern that should be adequately dealt with. The Working Group of Canadian Privacy Commissioners and Child and Youth Advocates in a report entitled: "*There ought to be a law: protection children's online privacy in 21st century*", offers insightful ways by which amendments can promote more

protection for children from internet-based media manipulations.[30] The implementation of federal legislation prohibiting the commercialization of advertising in children's online game and play spaces, the creation of online play spaces that are non-commercial are a few of the useful proposals from this report that can be considered.

(c) Data Breach Notification

Recommendation 7: *The Commission recommends that the Access Act and the Private Sector Protection Act be amended by the addition of an obligation to report to the Commission on security breaches that occur in public bodies and businesses and that involve personal information.*

Recommendation 8: *The Commission recommends that the terms and conditions be determined, leading to reporting of security breaches involving personal information.*

Recommendation 9: *The Commission recommends that it be entrusted with the power to order public bodies and businesses, on the conditions it determines, to notify the persons concerned by a security breach involving their personal information and to take the measures the Commission will deem necessary to ensure adequate protection of their personal information.*

22. CIPPIC is strongly supportive of the adoption of data breach notification obligations. The two-tier notification mechanism proposed in Recommendations 7-9 will be particularly affective, as it will avoid notification fatigue by not obligating individuals to be notified each and every time their personal information has been breached. At the same time, it prevents organizations from hiding behind overly high or subjective standards in order to avoid disclosing breaches in order to preserve good will.[31]

---

[30] 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", November 19, 2009, <http://www.gnb.ca/0073/PDF/Children%27sOnlinePrivacy-e.pdf>.

[31] T. Israel, "Bill C-12: Safeguarding Canadians' Personal Information Act – Eroding Privacy in the Name of Privacy", (2012) 9(5) Can. Priv. L.R. 45; (2012) 5(3) The Winston Report 5. Initial version available online at: Slaw Slaw.ca, March 23, 2012, <http://www.slaw.ca/2012/03/23/billc12-safeguarding-privacy-by-eroding-it/>.

23. We note that these obligations should involve a two-tier mechanism. First, all or close to all breaches or potential breaches of security safeguards must be reported to the Commission. Second, the Commission will determine which breaches need to be reported to affected individuals, as well as what remedial measures the reporting organization needs to adopt in order to address the breach.

24. Reporting to the Commission or any data protection authority will allow for an objective assessment of the severity of the breach and its implication on users privacy. Perhaps more importantly, it will encourage companies to adopt adequate technical safeguards, both in anticipation of a breach and after one has occurred, as when companies know they will be insulated from embarrassment by hiding an inevitable breach, there is minimal incentive to put in place the rigorous but often costly protections needed to safeguard private data in a digital age.[32]

(d) Accountability

Recommendation 10: *The Commission recommends that the Private Sector Protection Act provide for the creation of the function of person in charge of protection of personal information.*

Recommendation 11: *The Commission recommends that the function of person in charge in the private sector can be delegated by the business to a person working within the business.*

25. With regards to recommendation 10 and 11, the provision for a person in charge in the private sector is necessary to ensuring accountability and should be implemented. We note that the Federal, Ontario and British Columbia Privacy Commissioners have all recognized the importance of ensuring this type of accountability for businesses large and small alike.[33] All businesses should have a delegated individual in charge that can

[32] *Ibid*.
[33] Office of the Information and Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada & Office of the Information & Privacy Commissioner of British Columbia, "Getting Accountability Right with a Privacy Management Program", Last modified April 17, 2012, <http://www.gnb.ca/0073/PDF/Children%27sOnlinePrivacy-e.pdf>.

handles, monitors, and is held responsible for all affairs dealing with access to information and privacy concerns.

26. While the delegation of an individual in charge and other 'accountability' measures are all essential, it should be expressly emphasized that this is only one element of a successful data protection regime. Other elements, including obligations to minimize data collection strictly to what is necessary in order to achieve legitimate and reasonable objectives, and robust consent requirements, including technical interfaces designed with a 'privacy by default' mindset, are all additionally integral to any comprehensive response to data protection challenges.

II. The Right to Information: From Transparency to Open Government

27. In CIPPIC's view, access to information is a component of a broader right to receive and impart information.[34] We are encouraged by the leadership role Quebec has taken in open governance, transparency and open data initiatives, including concrete steps such as the implementation of Quebec's open data portal.[35] However, more can be done.

(a) Scope of Application

28. The Act's application is limited in scope. It fails to cover a broad enough range of bodies, a broad enough range of documents and a broad enough set of data storage scenarios.

29. To begin with, Quebec's *An Act respecting access to documents held by public bodies and the Protection of personal information* ("Quebec ATI Act"),[36] is deficient in its limited scope of application. While the Act applies to a broad range of 'public bodies', section 34 of the Act excludes members of the National Assembly from complying with access

[34] See Article 19, "International Standards: Right to Information", Policy Brief, 5 April 2012, online: <http://www.article19.org/resources.php/resource/3024/en/international-standards-right-toinformation>, text accompanying footnote 9.
[35] Government of Quebec, "Données Ouvertes", <http://www.donnees.gouv.qc.ca>.
[36] R.S.Q., c. A-2.1, <http://www.canlii.org/en/qc/laws/stat/rsq-c-a-2.1/latest/rsq-c-a-2.1.html>.

obligations unless they 'deem it expedient'.[37] This, for all intents and purposes, amounts to an exemption for members of the National Assembly as 'expedient' is sufficiently subjective and broad a standard to encompass anything, meaning members are not likely to disclose anything they would not disclose upon request if the Act did not apply to them at all.

30. Secondly, Quebec's right to information regime is overly limited in the records it applies to. Specifically, section 9 of the Quebec ATI Act excludes all ancillary information, such as outlines, drafts, preliminary notes, and so on.[38] In CIPPIC's experience, outlines, early drafts and preliminary notes provide vital insight into the development process behind key government documents and processes. It also adds important information on internal processes that is essential for transparency. This exception should be removed.

31. Finally, the Quebec ATI Act expressly excludes a right to access any data that would require processing before it can be released. This is problematic, as it precludes more cost-efficient solutions, particularly in scenarios where necessary data points are spread across several sources. This may not only lead to higher operational costs in responding to ATI requests, but may act as a deterrent to legitimate requests. The Centre for Law & Democracy, in its analysis of Quebec's right to information regime, describes it as such:

> This prevents users from getting information which a public authority holds, but which is spread across different documents or which needs to be extracted from a database. For example, if a requester wanted to know how much money an authority spent on a particular type of expenditure, and that expenditure was not specifically tracked, the authority would be justified in refusing the request, rather than totalling up their expenditures to find an answer to the question. This is obviously extremely problematic.[39]

[37] R.S.Q., c. A-2.1, section 34.
[38] R.S.Q., c. A-2.1, section 9.
[39] On this point, see: Centre for Law and Democracy, "Failing to Measure Up: An Analysis of Access to Information Legislation in Canadian Jurisdictions", September 2012, <http://www.law-democracy.org/live/wp-content/uploads/2012/08/Canada-report-on-RTI.pdf>, p. 8.

CIPPIC's experience with several federal and provincial ATI regimes confirms this. Cost is the most commonly used mechanism for narrowing the scope of a request – rarely, but at times, as a means of obscuring or deterring access to legitimate information. The obligation should be to provide the information sought in the most cost-effective and efficient manner.

32. Moreover, while a division between 'documents' and 'information' may have been justifiable in an earlier age when the underlying information did not exist already in databases, today assembling information should not pose great difficulties. Access to raw data would facilitate creative processes, app development, mashups, etc., and stimulate the technology sector in Quebec. The "studies" are valuable in themselves, and they should be published. But whereas government employees may have expended significant effort in analyzing the data themselves to produce a study, it seems counter-productive to require members of the public to spend time and effort extracting information from a document so as to perform their own analysis.

Suggestion 7: Remove the ability of certain government members to refuse an information request simply because they deem it expedient to do so.

Suggestion 8: Remove the exception for ancillary information found in section 9 of the Quebec ATI Act.

Suggestion 9: Remove the exception in section 15, removing documents that require computation or comparison of information in order to produce from the general right of access.

Recommendation 12: *The Commission recommends that the application of the Distribution Regulation be extended to the public bodies currently exempted.*

Recommendations 20: *The Commission recommends that the Access Act be amended to bring within the scope of the Access Act, all bodies having more than 50% of their joint stock held by the State.*

33. A number of public bodies included in the Quebec ATI Act are nonetheless excluded from the *Regulation respecting the distribution of information and the protection of*

personal information (the "Distribution Regulation").[40] These include Municipal bodies, School bodies, and Health and social services institutions.[41] The regulations also exclude the Lieutenant Governor, the National Assembly, and certain office holders. We see no principled reason why this should be the case. If they were excluded for financial reasons, the answer is that most of the documents for which distribution would be required already exists, and costs are obviously minimal given the extant portal infrastructure. Moreover, the same financial rationale applies to all public bodies, presently excluded or not: The costs of disclosure should be weighed against the concomitantly decreased scope for future ATI requests.

34. If there is a concern regarding privacy, as suggested by the exclusion of health institutions, then the answer is found in Division IV of the Distribution Regulations governing "Measures to Protect Personal Information". There seems to be no compelling reason, for example, why a school body should not be required to publish an "organization chart", as included bodies must under the Regulation.[42]

35. Second, the Quebec ATI Act should be applied to semi-public bodies carrying out public functions and activities. It is apparent that the range of bodies carrying out public functions has increased over the past decades, along with the scope of those functions. In some fields outsourcing has become the norm, with services being delivered by private entities which falling altogether outside the scope of provincial legislation.[43] It is therefore imperative that individuals have the ability to hold those bodies delivering public services to account, especially when it is clear that they are subject to at least partial governmental control or are reliant on public funds.

---

[40] *Regulation respecting the distribution of information and the protection of personal information*, R.R.Q., c. A-2.1, r. 2. <http://www.canlii.org/en/qc/laws/regu/rrq-c-a-2.1-r-2/latest/rrq-c-a-2.1-r-2.html>, section 2.
[41] *Regulation respecting the distribution of information and the protection of personal information*, R.R.Q., c. A-2.1, r. 2. <http://www.canlii.org/en/qc/laws/regu/rrq-c-a-2.1-r-2/latest/rrq-c-a-2.1-r-2.html>, section 2.
[42] R.R.Q., c. A-2.1, r. 2 ,sub- section 4(1).
[43] *Ottawa (City) v. Ontario (Information and Privacy Commissioner)*, 2010 ONSC 6835 [2010] 328 D.L.R. (4th) 171 (Ont. Div. Ct.).

36. In our view, the Quebec ATI Act should certainly apply to organizations with 50% or more government stock ownership or, rather, to any organization where the government is the largest individual stockholder. In fact, we would go further and suggest that its obligations be applied even to private entities, to the extent these are carrying out quintessentially public tasks at least in part at the direction, or by mandate of, the federal government.[44]

37. Important information should not be withheld *merely* on the basis of its source, but rather on consideration of the effects of its release. The right to information should be applied broadly, with narrow exceptions and the overriding public interest as the main touchstone animating disclosure.

> **Suggestion 10:** Extend the Disclosure Regulation to cover all public bodies.
>
> **Suggestion 11:** Extend the Quebec ATI Act to cover all entities in which the Government owns the largest amount of stocks.
>
> **Suggestion 12:** Consider applying the Quebec ATI Act to all entities performing essentially public functions by government mandate or at the government's direction.

(b) Open Governance & Data

Recommendation 13: *The Commission recommends that public bodies be subject to an enhanced regime of openness to government data, which allows free access to all government information useful to the public.*

Recommendation 14: *The Commission recommends that a public debate involving all partners (parliamentarians, individuals, associations, experts) be held to establish a model for an open Québec government, based on participation and collaboration.*

38. As we noted recently in our submission to the federal Office of the Information Commissioner's consultation on access to information: "government information

[44] *Godbout v. Longueuil (City)*, [1997] 3 S.C.R. 844, <http://www.canlii.org/en/ca/scc/doc/1997/1997canlii335/1997canlii335.html>.

should be viewed as a national resource and its generation, retention, processing and disclosure are paid for by taxpayers". [45] Or, as codified in the overriding objective clause of the Australian access to information regime:

> The Parliament also intends, by these objects, to increase recognition that information held by the Government is to be managed for public purposes, and is a national resource.[46]

In our view, the government obligation to proactively publish information of public importance is part of the broader democratic right to receive and impart information.

39. We note that some have stated concerns regarding a merger of broader proactive disclosure obligations with traditional access to information rights.[47] These rightly highlight that monitoring of proactive disclosure can be a time-consuming process that diverts scarce regulatory resources away from processing primary access to information requests. These critiques also raise concerns that individuals will have little or no input into the *types* of information to be released. The suggestion is that such obligations should be housed in a separate statutory regime, with a separate overseeing body. These concerns are valid, and should receive due consideration before the Quebec ATI Act's current proactive disclosure regime is significantly expanded.

40. Regardless of the specific mechanism, CIPPIC is of the view that an expanded proactive disclosure regime is needed. Information is the lifeblood of democratic discourse and transparency, of fact-based decision-making in general, and a host of downstream innovation leading to efficiency tools or 'apps', creativity and economic activity. The right to express one freely encompasses all of these levels of expression – democratic

---

[45] A Cooke & T Israel, "Bringing Canada's Lagging Information Rights into the 21st Century: Comments of the Samuelson-Glusko Canadian Internet Policy and Public Interest Clinic", 31 January 2013, <http://cippic.ca/uploads/OIC_Consult-Modernizing_ATI.pdf>, at paras 17-18.
[46] *Freedom of Information Amendment (Reform) Act 2010*, Act No. 51 of 2010 as am, <http://www.comlaw.gov.au/Details/C2012C00866>, sub-section 3(3).
[47] See, for example, M. Weiler, "Regarding Open Dialogue on the Access to Information Act", January 30, 2013, <http://www.oic-ci.gc.ca/eng/DownloadHandler.ashx?pg=be9c1298-43aa-4ba8-9869-a67fb3fc1e77&section=596721a2-8a78-4147-af09-4144e4556163&file=OD_DO_Mark_Weiler_Jan_30_2013.pdf>

discourse, truth-seeking expression, and personal self-expression. The right to *receive* information should as well.

41. The Disclosure Regulation, as currently crafted, imposes fairly robust disclosure obligations but these do not go far enough and raise potential concerns regarding resource strains, and the inability for individual input into which data sets should be proactively disclosed.

42. While the current Disclosure Regulation obligates the publication of responses to ATI requests that would be interesting to the public, an expanded proactive disclosure regime will, in CIPPIC's view, go further. Specifically, the Quebec ATI Act itself should obligate public bodies to *regularly* publish *up to date* information the distribution of which is of interest to the public. In addition, the Quebec ATI Act should give individuals the right to request certain categories or types of data to be produced regularly.

43. Additionally, the Quebec ATI Act should adopt a means for the Commission to levy administrative penalties against any public body that fails to meet proactive disclosure obligations. This will incentivize compliance and thereby reduce what might otherwise be a resource intensive regulatory oversight process. Additionally, as administrative monetary penalties are typically retained by the issuing regulator, this will further offset regulatory oversight costs.

44. This broader obligation to disclose proactively will also address a different drawback of the current Disclosure Regulation – its limited temporal application. Currently, there is no obligation to publish statistical reports, etc., produced prior to 2009. However, within this broader framework, earlier statistical and other datasets can be published if they meet publication requirements or are requested by individuals.

Suggestion 13: Adopt an expanded proactive disclosure obligation that encompasses all government data useful to the public.

Suggestion 14: Provide for a mechanism by which individuals may request data types be added to the list of proactively published information on a recurring basis.

Suggestion 15: Obligate information proactively published is provided in useful and interoperable formats. Allow for a right to request data be provided in a particular format, where feasible.

Suggestion 16: Provide the Commission with the power to impose administrative monetary penalties on public bodies that fail to comply with obligations under Quebec's ATI Act.

(c) The Time Limit to Justify a Refusal of Access to Information

Recommendation 15: *The Commission recommends that the Access Act be amended to specify that the time limit provided for in section 47 to respond to a request for access and justify a refusal to access on the basis of an optional restriction become mandatory and results in forfeiture.*

Recommendation 16: *The Commission recommends that a public body cannot be relieved from the consequences of the failure to invoke a reason for optional refusal within the mandatory time limit provided to respond to request of access except in exceptional circumstances, which it would have the burden of proving to the Commission.*

Recommendation 17: *The Commission recommends that the Private Sector Protection Act be amended to specify that the time limit stipulated in section 32 to respond to a request for access and justify a refusal on the basis of an optional restriction of access is mandatory and involves forfeiture.*

Recommendation 18: *The Commission recommends that a business cannot be relieved from the consequences of the failure to invoke a reason for optional refusal within the mandatory time limit provided to respond to request of access except in exceptional circumstances, which it would have the burden of proving to the Commission.*

45. There are clearly identified problems with the Act, whereby public bodies can evade clear statutory time limitations as well as their general responsibility to provide timely responses under the Act. As these loopholes allow for public bodies to effectively bypass clear statutory imperatives, we cannot believe that this outcome was intended

by the legislature. Timeliness is often critical to the effective and efficient processing of access to information requests, and these obligations should be mandatory.

(d) Exceptions & Limitations

46. It is our view that the overarching principle for excluding documents from publication should be whether it is or is not in the public interest to disclose and non-disclosure should moreover require proof harm. We therefore recommend that consideration of the public interest be added as an over-arching consideration in the assessment whether exceptions should be applied in any given instance, and that the need to demonstrate harm be adopted as a pre-requisite to evoking an exception.

> **Suggestion 17:** Adopt consideration of the public interest as an overriding factor in the assessment of all exceptions to disclosure.
>
> **Suggestion 18:** Mandate public bodies to demonstrate that harm will result if a disclosure occurs before relying on an exception in a given instance.

Conclusion

47. In sum, we are grateful for this opportunity to present our views on Quebec's privacy and right to information regime. We note that, in many instances, Quebec is a leader within Canada in the rules and protections it has adopted. However, as noted above, gaps continue to exist in both its privacy protection regime and in its open government obligations. In this respect, we hope our comments along these lines prove useful.

***** END OF DOCUMENT *****