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
https://cippic.ca

HOUSE OF COMMONS STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY & ETHICS (ETHI)

ORAL TESTIMONY OF THE SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY & PUBLIC INTEREST CLINIC (CIPPIC)

ON

CANADA'S AGEING *PRIVACY ACT*: THE NEED FOR MODERNIZATION

September 20, 2016

Tamir Israel, Staff Lawyer

Introduction

Thank you, Mr. Chair and members of the committee.

1. Good morning. My name is Tamir Israel, and I am Staff Lawyer with CIPPIC, the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic at the University of Ottawa's Centre for Law, Technology & Society and the Faculty of Law. CIPPIC is a public interest legal clinic that works to advance the public interest in policy debates that arise at the intersection of law and technology. I wanted at the outset to thank you for inviting us to testify before you today, as well as for undertaking this important review of the federal *Privacy Act*, a central component of Canada's privacy, transparency and accountability framework.

2. Since the introduction of the *Privacy Act* in the 1980s, the policy landscape surrounding data protection has evolved dramatically, driven by tectonic shifts in the technical capability and general practices surrounding the collection and use of personal information. The federal *Privacy Act* has simply not kept pace with these dramatic changes, a reality that hinders its ability to continue to achieve its objectives in light of heightened incentives and technical capacities to collect and keep personal information at unprecedented scale.

3. The nature of the objectives incentivizing state data practices have rapidly evolved over the years since the adoption of the *Privacy Act*, which initially focused primarily on regulating data practices animated by administrative purposes. Today's privacy challenges are driven by a far more diverse set of incentives. The era of data driven decision-making (colloquially referred to under the rubric of 'big data') increasingly pushes state agencies to cast wide nets in their data collection efforts. Additionally, more often than not the Act is applied in review of activities motivated by law enforcement and security considerations that arise in contexts far removed from the administrative activities that animated its introduction. Finally, data sharing between domestic and foreign state agencies now occurs on a more informal and often technologically integrated basis than could have been

envisioned in the 1980s.

4. The *Privacy Act* is in drastic need of modernization. To that effect, CIPPIC has reviewed and largely endorses the recommendations made by the Office of the Privacy Commissioner of Canada to this Committee with respect to changes necessary to ensure data protection challenges are met. We will elaborate on a number of these, as well as on some additional recommendations that we have developed in our comments today. In addition, in our written comments, which will submit to the Clerk for circulation to the Committee at a future date, we have provided some suggested legislative language in support of a number of our recommendations.

5. The remainder of our opening comments focus largely on discussing and highlighting specific recommendations designed to enhance proportionality, transparency and accountability, as well as to address shortcomings that have arisen from specific technological developments. Before turning to these broader themes, however, our first recommendation addresses the *Privacy Act*'s purpose clause, which we believe should be updated to explicitly recognize the objectives of the Act, namely to protect the right to privacy and to enhance transparency and accountability in the state's use of personal information. Express recognition of these purposes, as is done in provincial counterparts to the *Privacy Act*, will assist in properly orienting the legislation around its important quasi-constitutional objectives and will help to secure its proper and effective application if ambiguities arise in the future.

Recommendation 1: Update purpose clause

2. The purpose of this Act is to ~~extend the present laws of Canada that~~ protect the right to privacy of individuals and to enhance transparency and accountability with respect to personal information practices of ~~about themselves held by a~~ government institutions ~~and that provide individuals with a right of access to that information~~.

Necessity & Proportionality Measures

6. Necessity and proportionality are animating principles that have become central to data protection regimes around the world but are absent from the ageing *Privacy Act*. It is important to explicitly recognize these principles in the *Privacy Act*, and to adopt additional specific measures that are absent from its current purview, but are nonetheless essential to ensuring private data is collected in a proportionate manner.

7. As a starting point, the Privacy Commissioner's recommendation for explicit recognition of necessity as the standard governing data practices should be implemented. Necessity is a formative data protection concept and provides important context for assessing when data should or should not be collected, used or disclosed. The existing standard, which requires only that data practices relate directly to an operating program or activity, is simply too imprecise in the age of 'big data', where organizations are increasingly encouraged to collect data that has no clear immediate connection to current objectives.

Recommendation 2: Explicitly recognize necessity obligation

Collection of personal information

4. 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.

8. Second, the *Privacy Act* currently imposes no explicit limitations on how long data can be retained once it is legitimately collected. The lack of any explicit obligation to adopt reasonable retention limitations can mean that data is kept well beyond the point where its utility has expired, exponentially increasing the risk of data breach and of inappropriate uses. The lack of an explicit retention limitation requirement can even lead to the indefinite retention of data that has only short term utility, greatly undermining the proportionality of a particular initiative.

9. For example, our clinic recently issued a report with the Citizen Lab at the Munk School of Global Affairs which examines the use of a surveillance tool called a cell-site simulator. These devices operate by impersonating cell phone towers in order to induce all mobile devices within range to transmit certain information which is then used to identify or track devices or individuals. The devices operate in a coarse manner – for each individual target the devices are deployed against, the data of hundreds or thousands of individuals within range will be collected. Non-target data collected is only immediately useful for identifying which data belongs to the actual target and which does not, an objective which can be accomplished within 24 – 48 hours of collection. However, as the underlying collection of these thousands of non-target datasets is legitimate, these datasets might be kept indefinitely. These large non-target data sets can be re-used at any point in the future and, subject to ancillary statutory regimes such as the *Security of Canada Information Sharing Act*, recently adopted by Bill C-51, can be shared across a wide range of other agencies.

10. Including an explicit retention limitation provision would not only mandate state agencies to adopt clear retention policies, but would allow the Privacy Commissioner to address unreasonable retention in a principled manner. This, in turn, will reduce the risk of data breach and generally increase the proportionality of data collection practices.

Recommendation 3: Include Explicit Retention Limitation

Disposal of personal information

6. (3) Subject to (1), ~~A~~ a government institution shall dispose of personal information under the control of the institution once the personal information is no longer necessary for the operating program or activity for which it was collected and in accordance with the regulations and in accordance with any directives or guidelines issued by the designated minister in relation to the disposal of that information.

11. Third, we would recommend the adoption of an over-arching proportionality

obligation that would apply to all collection, retention, use and disclosure of personal information by government agencies into the *Privacy Act* that is comparable to that included in its private sector counter-part, PIPEDA. As you have heard from other witnesses, the *Privacy Act* increasingly provides an important avenue for ensuring *Charter* principles for the protection of fundamental privacy rights are fully realized. An over-arching reasonableness obligation modelled on sub-section 5(3) of PIPEDA would provide an avenue for assessing *Charter* considerations across all data practices and would ensure all practices are not only necessary in relation to legitimate state objectives, but also proportionate. It will also provide the *Privacy Act* with a measure of flexibility, allowing it to keep pace with technological change by providing a general principle by which unanticipated future developments can be measured.

Recommendation 4: Add Over-arching Proportionality Obligation

X. Personal information will only be collected, used, disclosed or retained by a government institution in circumstances and for purposes that a reasonable person would consider appropriate.

Transparency Measures

12. In addition to these proportionality measures, there are clear gaps in the *Privacy Act*'s current transparency framework and further opportunities to enhance the openness of state practices which, in turn, will encourage accountability and public confidence.

13. At the outset, we encourage adoption of the Privacy Commissioner's recommendation for a public policy override to the Act's confidentiality obligations. This would facilitate proactive reporting on privacy matters where it is in the public interest to do so, permitting public policy debates to occur in a timely manner.

14. Second, the *Privacy Act* should be amended to include statistical reporting obligations attached to various electronic surveillance powers found in the *Criminal Code*. Statistical reporting obligations were once a hallmark of electronic

surveillance authorization regimes and are encoded in Part VI of the *Criminal Code*. Part VI applies to activities such as wiretapping and video surveillance, which were once the cornerstone of law enforcement electronic surveillance practices. However, modern law enforcement has provided numerous additional sources of digital information. Current statistical reporting obligations have not kept pace, leaving an incomplete picture and undermining the public's ability to properly assess the scope of state electronic surveillance practices. Indeed, one investigation conducted by the Privacy Commissioner's office found that law enforcement agencies themselves did not have a clear idea of the scope of their own practices in relation to the collection of subscriber information from telecommunications companies. Understanding the nature and scope of state surveillance practices is all the more important in light of the tendency for rapid change in practices in this sphere. Imposing a statistical reporting obligation in the *Privacy Act* that applies across the spectrum of electronic surveillance powers would provide an important transparency mechanism.

15. Finally, the adoption of a general obligation on state agencies to explain their data practices would greatly enhance transparency. While the Act currently obligates government agencies to explain to individuals the purposes for which their personal information is collected and used, it lacks a general obligation to explain agency privacy practices. Adopting a general obligation to proactively explain privacy practices and to make additional information regarding such practices available to individuals upon request can provide an important avenue for further transparency and a window into government data practices. Such an obligation can be modelled on PIPEDA's openness principle, and would obligate government institutions to ensure individuals are able to obtain information regarding privacy practices without unreasonable effort.

16. This openness obligation should encompass a concept of algorithmic transparency. A growing trend by which algorithms are increasingly employed as central components of public and private sector decision-making raises

transparency and discrimination concerns. Where automated tools are used to parse large amounts of personal data in order to assist in government decision-making, the criteria underpinning resulting outcomes are often obscured. An openness obligation should therefore specifically include a right to understand the underlying logic of any automated decision-making tool.

Recommendation 5: Adopt an Openness Obligation

X. Government institutions shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about a government institute's policies and practices, including information relating to the underlying logic of any automated decision-making practices, without unreasonable effort.

Accountability & Compliance Measures

17. The *Privacy Act* can also benefit from measures designed to ensure general compliance with its precepts while enhancing state accountability in privacy practices.

18. We wish to highlight the importance of adopting the Privacy Commissioner's recommendation to formalize the obligation to undertake privacy impact assessments so that it has force of law. As this obligation already exists in theory, by means of Treasury Board directives, formalizing it will not be onerous. Explicitly including the obligation in the *Privacy Act* will ensure that the obligation is applied uniformly and to consistent standards. In addition, we would recommend the inclusion of a public consultation process within the Privacy Impact Assessment mechanism, so that public input can be sought in the formative stages of initiatives that have potential to be privacy intrusive.

19. In brief, we would also encourage the adoption of order making powers to the Privacy Commissioner as well as a formalized appeal path for all findings under the *Privacy Act*. This would not only facilitate a more timely resolution of complaints, but also improve the tenure of investigative processes by expressly recognizing the

regulatory nature of the *Privacy Act*. In addition, we would also encourage the extension of the Commissioner's research and education mandate, currently limited to private sector conduct under PIPEDA. As a final consideration, we would urge that the adoption of a private right of action coupled with statutory damages for egregious violations be explored as a means of further incentivizing robust and proactive compliance.

Keeping up with Technological Developments

20. Finally, we recommend a number of changes to the *Privacy Act* that are designed to address specific technological evolutions that have undermined its application in particular contexts.

21. First, we would recommend that the definition of 'personal information' be aligned with its counterpart in PIPEDA so that it is no longer limited in application to information that is 'recorded' by a government institution. Modern data collection and analysis practices can facilitate the use and even subsequent disclosure of personal information without the creation of any explicit 'record'. Yet privacy is nonetheless engaged. A definition limited in application to expressly recorded data is therefore out of step with modern data practices.

Recommendation 6: Update definition of personal information

3. *personal information* means information about an identifiable individual ~~that is recorded in any form~~ including, without restricting the generality of the foregoing

22. Second, an explicit obligation to adopt reasonable technical safeguards must be imposed in the Act. High profile data breaches have become common, and government agencies are far from immune. Last year, the United States Office of Personnel Management experienced a data breach estimated to have affected 18 million individuals, and attributed by the US Office of the Inspector General to persistent deficiencies in data security practices. Minimizing the collection and retention of personal data can reduce the impact of data breaches. However, it can

be anticipated that government networks will be ongoing targets in the future. Imposing an explicit obligation to adopt reasonable technical safeguards will permit the Office of the Privacy Commissioner to leverage its growing expertise in data security and facilitate the adoption of more rigorous data security standards.

Recommendation 7: Add explicit obligation to adopt technical safeguards

X. Government institutions shall adopt reasonable security safeguards to protect personal information against unauthorized access, disclosure, copying, use or modification.

23. Finally, we would endorse the recommendation of the Privacy Commissioner and others to adopt a data breach notification obligation in the *Privacy Act*. Such reporting already occurs informally. However the absence of a legal obligation in the *Privacy Act* will encourage uniform notification practices, while allowing the nature and scope of such breaches to be consistently monitored by the Office of the Privacy Commissioner.

Those will be my opening comments for today. As I mentioned at the outset, we will be submitting a written version of these comments with supplementary recommended legislative language to the committee at a future date.

Thank you.

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