Public Interest Advocacy Centre (PIAC)

John Lawford, Executive Director and General Counsel
Alysia Lau, Legal Counsel

Written notes for an oral submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics

Review of PIPEDA

Ottawa, Ontario

February 14, 2017

1. The Public Interest Advocacy Centre (“PIAC”) is a national, non-profit organization and registered charity that provides legal and research services on behalf of consumer interests, and, in particular, vulnerable consumer interests, concerning the provision of important public services. We have been deeply involved with the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") from a consumer perspective since before its passage.

2. Five years ago we came to talk to this Committee about privacy and social networks. Today we come to discuss your review of PIPEDA: and it is still about social media, but this time it has brought along its friend, big data.

Personal Information and Consent in the Age of Big Data

3. Social networks and most smartphone apps routinely gather personal information as defined by PIPEDA and retain that information on central servers. That information is then used, as is permitted by PIPEDA, to target advertisements to that person and also to their related friends, families and colleagues on social media. The term for this is behavioural advertising or marketing, as the vast amounts of very personal data, including one's preferences as to a myriad of products, previous purchases, location, age, gender, ethnicity and much more, allow the advertisers using this information to target these ads to your presumed behaviour and profile.

4. They call it "big data" when advertisers or other companies are able to combine data sets from various apps and website visits and even from only one site over a long period. Then "data mining" occurs – using algorithms to look for patterns that suggest how successful targeting ads may be – or even attempting to find presumed ways to know or influence your future behavior.

5. The companies doing this will tell you today that they are doing it lawfully under PIPEDA: they have privacy policies; they have your consent; they follow all of the rules about sharing and processing data.

6. The fact is that they often do not have your informed consent. Informed consent, where you understand the consequences of the provision of your information and what it will be used for, and how it will be shared, is the standard for collecting, using or disclosing information under PIPEDA.

7. Companies now are asking that the consent standard be changed, largely because it impedes the data gathering that big data requires. They will ask you to abandon informed consent as the standard that protects consumers and their reasonable expectations of, and conceptions of, privacy. They will ask for a "risk-based" model or more "implied consent". This should be resisted. Indeed, PIPEDA needs to enable the informed consent standard and even needs to add some new rules to protect consumers.

Enforcement

8. To address the problems with online privacy and big data, the Privacy Commissioner of Canada needs real enforcement powers including a mandatory order-making power and an "AMPs" or fining power.

9. PIAC advocated for these powers at the first PIPEDA review in 2008. The OPC at that time did not want them. Then the OPC crossed swords with Facebook over a complaint in 2010. After that, Jennifer Stoddart asked you and the government repeatedly and loudly for order-making and fining

powers. Her reasoning was that her office could not make large social media companies comply with only non-binding "findings" and "name and shame".

10. Mr. Therrien, the present Privacy Commissioner, is more careful, and may ask you only for order-making power. This will be cumbersome to enforce in court. He should also be given a fining power. In any case, if the Privacy Commissioner says he or she needs it to do the job, why not give it? The OPC is up against the biggest corporations in the world now – and needs tools. It is embarrassing that provincial Commissioners have this power not the OPC. Only by enforcing the present standards in PIPEDA can we see if they are effective or need change. It is unfair to judge the Act otherwise.

Children and PIPEDA

11. A particular new rule needed is regarding the treatment of children's privacy. I saw an extraordinary op-ed last week. In it, Owen Charters, president and CEO of the Boys and Girls Club of Canada said:

> The Wall Street Journal reports that popular children's websites in the U.S. install more tracking software than sites aimed at adults. These tracking tools follow our children as they surf the web, collecting data about their behaviour and interests. This information is often sold to marketing companies.
>
> There are endless public awareness campaigns dedicated to cyberbullying. Change is happening. But with the focus on those discussions, children's privacy rights in Canada have been placed on the back burner.

12. That a general children's welfare charity would underline online privacy as a problem is telling. The letter closes with an exhortation to the Canadian government to pass a dedicated children's privacy act.

13. Our sentiments are similar but we think this protection can be added to PIPEDA. We have first-hand insights on the problem.

14. In 2011, PIAC brought a privacy complaint against Nexopia.com Inc., a social network based in Alberta and largely aimed at a teen audience. The Office of the Privacy Commissioner (OPC) upheld all our complaints, which were focused not so much on online safety but on targeted marketing to minors.

15. Unfortunately, besides some voluntary guidelines from the OPC, we see no improvement to children's privacy in Canada online since then. We have a detailed proposal to address this and Europe is adding regulation, but given our time to present, we invite you to ask us about these solutions in questions.

Data Retention & Destruction

16. Another area that requires a new rule is data retention and destruction. Can consumers in the future be sure that information that they provided – or that was extracted from their habits – will be destroyed or no longer used when the reasons why they gave that consent are gone? Will they have control?

17. Some of those present today would say no. We say now is the time to erase.

18. PIPEDA states personal information must only be retained for as long as necessary to fulfill an organization's stated purpose. However, the Act only requires organizations to develop guidelines and implement procedures regarding the retention of personal data, and says that personal information that is no longer required to fulfill the stated purposes "should" (not "shall") be destroyed, erased, or made anonymous. This is not strong enough.

19. The only OPC findings that Nexopia refused to implement – to the point of being taken to court by the OPC – were those requiring them to erase personal information of teens who had left their service.

20. As Canadians can now spend years, decades – and in the case of children, possibly their entire lives – on an online service such as a social networking website, the amount of personal information collected from a user could be staggering. And the more information on individuals an organization has, and the longer they keep it, the greater and more serious the risk of a data breach.

21. Canadians must have choice and control over the ways their personal data is used—including through consent, rectification of information, and especially removal or erasure of their information.

22. A right to erasure was recognized in the European Union's recent General Data Protection Regulation (coming into force in 2018). The new GDPR codifies what is known as the "right to erasure". This gives individuals the right to have personal data erased and to prevent processing of their data when, for instance, the individual withdraws consent or objects to the processing and there is no overriding legitimate interest for continuing it. Organizations are also required to be particularly sensitive when it comes to personal data shared by children on, for instance, a social networking site. They can only refuse to erase personal data when requested in certain circumstances, such as to comply with legal obligations or exercise freedom of expression.

23. PIAC submits the Committee should consider recommending similar rules for PIPEDA which would align with the GDPR's protections. For instance,

organizations should be upfront with users about how long they intend to retain their personal data and why. They should also be required to erase or destroy personal information once the data is no longer needed for a stated purpose or when an individual withdraws consent.

Final Thoughts for the Future-Proofing of PIPEDA

24. In our 2012 remarks, we suggested: "related party" tracking and reporting of data flows; a "Do Not Track" list; and "Privacy Impact Assessments" for social networks and other businesses before they launch services using personal information.

25. In our recent submission to the OPC on the question of interpreting consent in the online context, we suggested implementation of standard privacy preferences and a trustmark system.

26. We urge the Committee to consider such forward-looking questions of how to support the present PIPEDA informed consent standard – as Canadians grapple day-to-day with the consequences of targeted marketing and big data.

Conclusion

27. PIAC thanks the Committee for this opportunity to speak to you today and we are happy to answer any questions from you.