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

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

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

ON

ETHI STUDY: PRIVACY & SOCIAL MEDIA

June 19, 2012

Tamir Israel, Staff Lawyer

Introduction

Good morning. My name is Tamir Israel, and I am staff lawyer with the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC). CIPPIC is grateful for this opportunity to present its views on the privacy implications of social media to this Committee.

CIPPIC is a legal clinic based at the University of Ottawa's Centre for Law, Technology & Society (CLTS). We advocate in the public interest on issues arising at the intersection of law and technology. Since its inception, CIPPIC has taken an active part in legal and policy debates surrounding online privacy, both domestically and internationally. Our clinic filed the complaint that led to the first comprehensive investigation of an international social network's privacy practices.

The growing importance and benefits of social media to Canadians cannot be understated. These are far-ranging, and permeate every aspect of our individual, social and political lives. The innovative and commercial growth of such networks should not be unduly restricted. At the same time Canadians should not be forced to choose between their privacy rights and their right to participate in this new interactive world.

PIPEDA, which forms the backbone of privacy regulation in Canada, provides a flexible set of principles that caters to the legitimate needs of businesses while providing safeguards for user privacy. While PIPEDA has largely withstood the test of time, the privacy landscape has changed substantially since its enactment and a decade of experience has exposed a number of shortcomings that should be addressed if the statute is to continue to meet its objectives.

I will quickly say a few words about the shifting privacy landscape, then proceed to elaborate on four areas that I think need immediate attention. I will close with brief reference to a number of other issues that warrant further examination.

In her recent testimony before this Committee, Professor Valerie Steeves pointed to research indicating growing lack of trust in online companies. A survey conducted for Natural Resources Canada in late 2009 similarly found that "Respondents' level of trust in different types of organizations to keep their personal information secure is moderate to low...The least trusted were small private sector businesses (15%) and social networking sites (6%)." The study similarly found that the ability to control the context in which information is shared increased levels of trust. In another study conducted by researchers at Annenberg and Berkley, 67% of Americans agreed or strongly agreed that users "have lost all control over how personal information is collected and used by companies."

Feeding this 'sense of lost control' is an increasingly complex ecosystem where the scope and nature of data collected increases daily, even as the sophistication of information collection and analysis mechanisms keeps pace. While Google and Facebook have been at the forefront of debates on these issues, there are numerous companies involved.

Acxiom, a data broker based in Arkansas, has reportedly collected an *average* of 1,500 data points on *each* of its 500 million active user profiles. Few of these users have heard of Acxiom, let alone had any direct interaction with the company. Yet the profiles which data brokers such as Acxiom sell are populated with their browsing habits, the Facebook discussions they have with their friends and family, their sensitive medical and financial information, their ethnic, religious and political alignments and even on real world locations visited. All this data is collected, analyzed and refined into a sophisticated socio-economic categorization scheme, which Acxiom's customers use as the basis of decision-making.

The sheer complexity of the ecosystem that fuels databases such as Acxiom's defies any attempt to articulate within the confines of a privacy policy. A number of jurisdictions are looking at ways of addressing the need for greater transparency and choice. I will briefly highlight four here.

Needless to say, the nature of the data being collected is also increasing in sensitivity. Newly emerging capacities are aiming to incorporate real-time location and even emotional state.

Transparency

First, greater transparency is needed. To this end, the U.S. Federal Trade Commission has recently stated it will push data brokers to provide centralized online mechanisms that will help users discover which data brokers have collected their data. This can serve as the basis for the exercise of other user rights.

Informing users can be achieved through greater integration of notification into the service itself. This not only allows for greater flexibility and nuance in notification, but also increases privacy salience by reminding users in context of the privacy decisions they are making.

In addition, elements of privacy policies can be standardized, but care must be taken not to oversimplify data practices that are in reality complex. The dangers of oversimplification is that organizations will begin to rely on blanket and categorical consent which are simple, but do not provide customers or advocacy groups the details they need to properly assess their practices.

Privacy by Effort

Transparency alone, however, is not enough. In a recent consultation process on online privacy, it was noted that many online services are "public by default, privacy by effort". New users will rarely know how to configure the complex web of often conflicting privacy controls services offer when first signing on. Settings constantly shift and change as new ones are introduced and old ones replaced or when new features are added to existing services. Simply maintaining a constant level of privacy is a never-ending effort.

Compounding such efforts is the tendency for social networking sites to make occasional tectonic shifts in the constitution and nature of their services. These are often imposed on

engrained users as 'take it or leave it' propositions. At other times, pre-selected defaults are used to 'nudge' users in directions that are very different from the service they have grown accustomed to.

As you have heard from other experts – the devil is indeed in the defaults. Stronger protections are needed to ensure new services and settings are introduced with privacy friendly defaults that reflect the expectations of users and the sensitivity of the data – not whatever configuration best fits the service provider's business model.

Under PIPEDA, the form of consent should already be tailored to user expectations and the sensitivity of the data that might be affected. However, in order to firmly engrain this concept in service design, 'privacy by default' should be explicitly adopted as a principle under PIPEDA.

Enforcement and Process

The Committee has heard from a number of parties about the importance of ensuring the Office of the Privacy Commissioner can enforce its powers. Adding 'bite' to PIPEDA is critical for a number of reasons. First, it is necessary in order to provide incentives for compliance. Currently, there are very few as the penalties for non-compliance are few or non-existent. In most cases, the most an organization can expect is the threat of being publicly 'shamed' for non-compliance.

Second, having these powers will assist the Office of the Privacy Commissioner in its interactions with large multi-national organizations so that it can carry out its mandate in protecting the privacy of Canadians.

In addition to adding penalties, procedural changes to the OPC's investigative and compliance framework should be explored. Compliance with OPC recommendations in a social networking context may be a long and complicated road requiring changes to system design. However, under PIPEDA, the OPC's legal mandate to exercise its powers over a particular complaint ends 45 days following the issuance of an official Finding. This mechanism lacks the flexibility necessary to ensure OPC recommendations are carried out adequately.

Breach Notification

A final brief word on breach notification. Canada is in dire need of a breach notification obligation. Such an obligation will improve incentives to build stronger technical safeguards and provide users with opportunities to redress harms such as identity theft and humiliation that may result from a breach of their data.

Bill C-12 provides a workable framework for breach notification, but requires fixes and a commitment to introduce penalties for non-compliance if it is to be effective.

I would be happy to elaborate further on any of these points, and CIPPIC plans to file a more detailed brief with the Committee at a later point.

Thank you very much for your time and attention. I would be pleased to take your questions.

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