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

STUDY: GROWING PROBLEM OF IDENTITY THEFT AND ITS ECONOMIC IMPACT

June 3, 2014

Tamir Israel, Staff Lawyer

Introduction

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

1. Good afternoon. My name is Tamir Israel, and I'm staff lawyer with the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC). CIPPIC is very grateful for this opportunity to provide our input into this important study on the growing problem of identity theft and its economic impact. I'll cut my comments a bit short, given the time constraints.

2. In many ways identity crime is the crime of the information age. The U.S. Federal Trade Commission's Consumer Sentinel Network collated and classified over two million consumer complaints in 2013, and identity theft complaints comprised the top category across all these. Identity theft is a vehicle for a range of identity crimes. The false identities built on this theft are used to procure fraudulent loans, government benefits, and credit cards. These false identities are also used as a jumping off point for other crimes. As a result, the economic and social costs of identity crime remain difficult to measure.

3. In spite of these difficulties, it is safe to say that identity theft is on the rise. Identity theft 2.0 is taking hold, where identity thieves take full advantage of the rich information stores available on social media and mobile devices with increasingly savvy methods. Illegal online markets for identities have developed where e-mail account access, credit card numbers, and full identity profiles can be bought and sold en masse. The OECD estimates that lists of valid e-mail addresses can be purchased at between $1.70 U.S. to $15 U.S. per megabyte, and that in 2009 access to compromised e-mail accounts ranges from $1 U.S. to $ 20 USD, depending on the black market fluctuations.

4. Putting aside the economic costs, however, the most insidious impact of identity crime is on the individual who's the victim of identity crime. The time, effort, and trauma involved in recovering from identity crime cannot be easily measured in economic terms.

5. In the remainder of my comments I'll address three essential and necessary components of any comprehensive response to the problem of identity theft. They are prevention, research and education, and victim support. Before turning to these I wish to speak briefly about another essential component, which is investigation and enforcement.

6. We've done a lot in Canada to improve the ability of our various agencies, including the Office of the Privacy Commissioner of Canada, the Competition Bureau, and our various law enforcement agencies, to investigate identity theft as well as to address many of the underlying offences that facilitate identity theft. These initiatives include the addition of several Criminal Code provisions and the passing of S.C. 2010, c. 23, which is Canada's Anti-Spam and Spyware Legislation (CASL). These steps have been critical, but it's important to recognize that identity theft is here to stay, and an enforcement solution alone will not be enough to address the

problem. With that, I turn to some of the other solutions that are necessary to supplement what we've already done in Canada.

Prevention

7. First and foremost, more needs to be done to help individuals protect their identity information so that it doesn't end up in the hands of identity thieves in the first place. The most effective way to do this is through stronger data protection frameworks, including a stronger PIPEDA and Privacy Act.

8. PIPEDA in particular needs to play a central role in any comprehensive response to identity crime. Partaking in the many benefits of the digital age necessarily entails entrusting significant amounts of personal data to third parties. Today's social networks and mobile devices are an immense repository of information, but this information is often disclosed in unexpected ways, be it to the general public or to invisible third-party applications. PIPEDA is the only tool that can assist individuals in this context – by obligating organizations to gain meaningful consent for data practices and to limit their collection, retention and disclosure of personal data.

9. PIPEDA also obligates organizations to put in place reasonable technical and other safeguards in order to prevent unauthorized access to customer data. Security breaches are not only becoming more frequent with each passing year, but the number of identities exposed with each breach is increasing dramatically. Symantec's 2014 Internet Security Threat Report registered a 260% annual increase in the number of identities exposed by each average breach, meaning that large repositories of data are being increasingly targeted as a 'one-stop shop' source of identity data. This makes the adoption of strong technical safeguards a very important tool in the prevention of identity theft.

10. Against this backdrop the need for a PIPEDA framework that is rigorously enforced and applied has never been greater. However, no such framework is in place. Simply put, PIPEDA lacks the most basic enforcement and penalty mechanisms that are a hallmark of all other regulatory regimes in Canada and of most other data protection statutes around the world and in the Provinces. As this committee recognized in its recent study on privacy and social media in the age of big data, quoting former Privacy Commissioner of Canada Jennifer Stoddart:

> *With the emergence of Internet giants, the balance intended by the spirit and letter of PIPEDA is at risk, and the risk of significant breaches and of unexpected, unwanted, and even intrusive use of people's information calls for commensurate safeguards and financial consequences not currently provided for in PIPEDA.*

Bill S-4, currently before the Senate, takes an incremental step towards making PIPEDA somewhat more enforceable by providing for optional consent orders. However, full enforcement powers and administrative monetary penalties for non-compliance are required, so that companies have effective incentives to comply proactively with PIPEDA's obligations.

11. Bill S-4 will also enact far overdue breach notification obligations. These will obligate companies to report any privacy breaches that raise a real risk of substantial harm to affected individuals and to the Privacy Commissioner of Canada. A company that fails to disclose will be guilty of an offence and subject, upon summary conviction, to a fine of up to $10,000. While the breach notification obligation in Bill S-4 is a positive step forward, it is not sufficiently calibrated to deter security breaches. It focuses too closely on the risk of direct harm to an end-user resulting from a specific breach. In reality, in many instances it will be difficult to know whether a particular vulnerability was or was not exploited, meaning that much laxity in technical safeguards will remain unreported. This makes it an ineffective mechanism for encouraging and incentivizing companies to adopt sufficiently protective technical safeguards.

12. Recently a number of government departments have also seen high-profile breaches. These have included, for example, a breach at Human Resources and Skills Development Canada (HRSDC) involving a hard drive that contained sensitive information for over 500,000 students who had applied for student loans. In spite of this increase in breaches of government-held data, the *Privacy Act* continues to lack not only a breach notification obligation but also the basic obligation to adopt reasonable technical safeguards.

Research and Prevention

13. I'll turn now to research and education. In addition to prevention, a comprehensive response to the problem of identity theft requires education and outreach initiatives. A number of government agencies have developed some solid identity crime-specific consumer education materials. The Competition Bureau's “Little Black Book of Scams” is a good example. It's available online if anybody wants to take a look. These are supplemented by growing efforts from non-governmental bodies such as the Canadian Identity Theft Support Centre, whose Victim Toolkit is an excellent resource. But more can be done to educate Canadians on the hazards of identity theft and also to provide them with the increasingly sophisticated skills needed to protect their personal data and identities in the digital world.

14. There is also a need for coordinated and sustained research on the scope and parameters of identity theft. There has been minimal systematic research on this within Canada since about 2006, primarily due to a lack of sustained funding. While there are some non-Canadian initiatives that provide some insight into the scope and parameters of the problem within Canada, there is a need to stimulate and coordinate more Canada-specific research on identity crime through an initiative such as the breach repository that my colleague Kevin Scott mentioned earlier.

Victim Support

15. Finally, I turn to victim support, and I'll make this brief, because my colleagues here from the Canadian Identity Theft Support Centre did an excellent job of outlining many of the

elements that are necessary for an effective victim support framework. Many of my comments overlap with theirs, so I'll just make this brief.

16. The recovery process for an identity crime is highly complex. Victims must deal with creditors who are reluctant to believe their debt is not theirs. Even if a victim is successful in convincing immediate creditors, bad credit ratings can follow victims of identity crime for years. A number of steps can be adopted to mitigate these problems. For example, a customer seeking to convince creditors she is a victim of identity crime will often need to undergo completely diverse and complex processes for each provider in order to prove her identity. Often these will require different documentation, and this greatly multiplies the hours it takes to recover one's identity. In this vein, the type of standardized documentation provided by entities like the Canadian Identity Theft Support Centre is crucial. It's also crucial to make sure that it's recognized by both law enforcement and service providers as an acceptable means of providing documentation of identity theft. Other useful and necessary tools would be the availability of cost-free credit freezes and online access to credit reports, which this committee heard about earlier.

17. Finally, the ongoing availability of a victim support centre is essential to the overall recovery process. Having someone to talk victims through the identity recovery process and to assist them in their dealings with law enforcement and other agencies as well as with creditors is essential.

18. Overall, a national strategy on identity theft victim support should be adopted that will establish clear parameters for cooperation between the various entities involved in the victim support process, such as the Canadian Anti-Fraud Centre, the Canadian Identity Theft Support Centre, and the various regulatory agencies that deal with identity theft matters. It should also establish a clear road map for adopting these various identity recovery mechanisms.

Thank you.

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