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 INDUSTRY, SCIENCE & TECHNOLOGY (INDU)

RESPONSE TO FOLLOW-UP QUESTIONS OF THE SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY & PUBLIC INTEREST CLINIC (CIPPIC)

ON

BILL S-4: DIGITAL PRIVACY ACT

March 24, 2015

Tamir Israel, Staff Lawyer

INTRODUCTION

1. The Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC) at the University of Ottawa's Centre for Law, Technology & Society is pleased to provide this additional response to follow up questions regarding Bill S-4, the *Digital Privacy Act*. CIPPIC appeared to testify on this matter on February 19, 2015. Our appearance was regrettably cut short by Parliamentary scheduling conflicts and we have been graciously invited by the NDP members of this Committee to respond to some follow-up questions in writing. We do so below.

Question 1: The title of this Bill, *The Digital Privacy Act*, implies that protecting the privacy of Canadians is the goal of this bill. However, there are multiple new scenarios in which businesses can share personal information with each other including during prospective business transaction, and in the case of investigating if a contravention of law may be committed. Do the proposed amendments strike a balance between protecting Canadians' privacy and allowing businesses the freedom to conduct their due diligence?

2. Bill S-4 introduces a few key privacy protections. These include a more robust concept of consent and an obligation to notify individuals of a breach of security safeguards where the the breach poses a real risk of significant harm to affected individuals. In addition, Bill S-4 adopts some welcome procedural mechanisms such as an extended appeal period and the ability for the Privacy Commissioner to enter into binding consent agreements. It is regrettable, however, that Bill S-4, the Digital Privacy Act, introduces problematic exceptions as well. Indeed, Bill S-4 introduces far more exceptions to privacy protection than actual protections. Although we do not take issue with many of these, they provide businesses with significant latitude in a number of contexts and, as a result, speak to the overall balance of the Bill.

3. **Investigation Exception.** The most problematic of these is an exception that will permit private companies such as Internet Service Providers and Banks to hand over any customer information on request to any other private organization conducting a current, prospective or preventative investigation. The exception only applies where it is expected that seeking knowledge or consent of the affected customer might compromise the investigation. However, there are few situations where an ISP customer would consent to allowing their would-be accuser access to their information. In this regard, any investigation could be compromised by an anticipated lack of consent, meaning that this exception could almost always apply in the situations where judicial safeguards are most needed. Many of the legal protections adopted by

the courts as a pre-requisite to these types of third party disclosures are specifically designed to prevent plaintiffs from accessing this type of information in an abusive fashion.

4. These safeguards are designed to prevent abuse and have been used by the courts to ensure ISP customers are not unduly accosted by copyright trolls for their alleged anonymous online activities, to protect the authors of anonymous online discussions from being identified without a court first deciding the comments have broken some law, and to ensure anonymous whistleblowers are not identified without first confirming that there is an actual intention to sue for a breach of some law.

5. Since Canada lacks the intermediary liability protections available to online platforms in the United States, it has become fairly common to threaten the website or ISP holding the information sought with a lawsuit if they refuse to provide the identifying information in question. CIPPIC has seen numerous examples of this over the years in the digital context. Many have resulted in harm to anonymous end users while others have harmed online platforms by pitting them against their customers under threat of costly lawsuit. As PIPEDA does not impose any meaningful prospect of penalties if the company faced with this demand mis-interprets the scope of the exception and hands over customer information without justification, the incentive to err on the side of disclosing is significant. Harm to end users will ensue if this exception is adopted in its current format. Nor is there need for this exception. The courts have mechanisms for discovery that allow companies to access information they legitimately require for investigation of legal wrongs.

6. We acknowledge current problems with respect to the accreditation of investigative bodies such as professional societies, but these issues could be easily addressed in a much more balanced manner without raising all the ancillary harms implicated by Bill S-4. This could be done by replacing the current proposed exception with one focused on defining the entities that can rely on it, not the activities it permits. This could involve a functional definition of true professional regulatory bodies. Such a definition can be found in sub-section 2(k.1)-(k.2) of Alberta's *PIPA*. A broader definition, inclusive of other legitimate investigatory bodies, would be acceptable, but the current exception, which applies to any individual or company, is far too broad.

7. **Mandatory Disclosure to the State.** A second troubling and potentially far-reaching information-sharing mechanism that could have serious implications for Canadian privacy is found in Clause 10 of Bill S-4, which seeks to enact sub-sections 10.2(3) and (4) of PIPEDA, a

mandatory and open-ended disclosure obligation. Under this provision, companies who experience a breach are obligated to provide detailed information to an open-ended list of government and private sector organizations. When Bill S-4 was first drafted, several years ago, this provision would likely have applied primarily to credit companies, banks or other financial reporting entities able to take ameliorative actions on behalf of their customers. However, cyber-threats have evolved to include several other entities with shared security mandates, granting public safety and other investigative organizations such as CSE and the RCMP a significant role in cyber threat harm reduction. However, no correlating safeguards have developed to demarcate the lines between the defensive activities of these entities and their offensive activities. Indeed, steps have been taken to erode any such demarcation. At the same time, digital breaches can be extremely far-reaching, implicating immense amounts of highly sensitive data. This has rendered challenging efforts around the world to strike the appropriate balance when establishing frameworks to govern the exchange of data between private companies and the government in the context of a breach of safeguards.

8. Attempts to establish cyber-security information sharing regimes have proven challenging. In 2013, the White House committed to using a rare executive veto to prevent H.R. 3532, the *Cyber Intelligence Sharing and Protection Act* from becoming law. This committment was in part due to the expansive and one-sided information sharing provisions of CISPA and for the expansive role envisioned for intelligence-agencies (such as CSE's US counterparts, the NSA):

> … the bill would allow broad sharing of information with governmental entities without establishing requirements for both industry and the Government to minimize and protect personally identifiable information. … The bill also lacks sufficient limitations on the sharing of personally identifiable information between private entities and does not contain adequate oversight or accountability measures necessary to ensure that the data is used only for appropriate purposes. Citizens have a right to know that corporations will be held legally accountable for failing to safeguard personal information adequately. … H.R. 3523 effectively treats domestic cybersecurity as an intelligence activity and thus, significantly departs from longstanding efforts to treat the Internet and cyberspace as civilian spheres. [1]

[1] https://www.whitehouse.gov/sites/default/files/omb/legislative/sap/112/saphr3523r_20120425.pdf

The cyber-security information-sharing regime adopted in Bill S-4 replicates many of these problems. It obligates companies to notify any private or government body capable of reducing the risk of harm resulting from a given breach. Increasingly, there will be pressure to include policing and intelligence bodies such as CSE in this list. It then grants companies an open-ended exception to disclose any customer information for the general purpose of reducing or mitigating harm from a breach.

9. Often, in an ongoing breach situation (as is common with cyber breaches), this would involve direct data sharing with intelligence agencies with a cyber defence mandate. Yet Bill S-4 makes no attempt to ensure only necessary data is disclosed, that it is anonymized to the greatest extent possible before sharing occurs, that the data will be destroyed by the receiving agency once it is no longer required or that the data will not be used for any other purposes. Bill C-51 will remove barriers to sharing of cyberseucrity information between government agencies, further exacerbating the problem. The emails, bank accounts or private cloud data of thousands of Canadians can be implicated by a single breach, leading to wide-ranging potential for customer information sharing without adequate safeguards.

10. Importantly, this provision is not required. As it only applies to instances where affected customers must already be notified of a breach, the knowledge and meaningful consent of customers could be easily obtained as a pre-condition to any such disclosure. As the measures proposed are for the benefit of the individuals in question, presumably it should not be difficult to obtain consent unless the proposed disclosure is excessive in scope. Finally, where disclosure is necessary to prevent a risk of harm to life, health or security of a particular individual, companies can already rely on paragraph 7(3)(e) of PIPEDA. We believe this was not the intended application of sub-sections 10.2(3) and (4) of Bill S-4, which were drafted several years ago before this complex cybersecurity paradigm became a reality. Nonetheless, we are concerned that once enacted, it will be used to violate the privacy of Canadians unnecessarily. The Bill would therefore be more balanced if these sub-sections were removed.

11. **OPC Regulatory Regime.** The privacy protections proposed by Bill S-4 could go much further, and fail to address long-standing problems inherent in Canada's regime for protection of privacy. The lack of an order-making and administrative monetary penalty capacity in particular trivializes the entire regulatory regime and, as years of experience have demonstrated, is a direct hindrance to the Office's ability to carry out its mandate. As far back as 2010, two independent

experts reached this conclusion after conducting a comprehensive audit of the OPC's regulatory context.[2] The situation has gotten significantly worse since then, and the lack of true regulatory powers has seriously hindered the OPC's ability to carry out its mandate. We point you to the testimony of former Privacy Commissioner of Canada Jennifer Stoddard and former Assistant Privacy Commissioner of Canada Chantal Bernier before your sister committee, ETHI:

> ... the balance intended by the spirit and letter of PIPEDA is at risk. The quasi-monopoly of these multinationals has made PIPEDA's soft approach, based on non-binding recommendations and the threat of reputation loss, largely ineffective, I believe. We have seen organizations ignore our recommendations until the matter goes to court. We have seen large corporations, in the name of consultation with my office, pay lip service to our concerns and then ignore our advice. Moreover, with vast amounts of personal information held by organizations on increasingly complex platforms, the risk of significant breaches and of unexpected, unwanted, or even intrusive uses of that information calls for commensurate safeguards and financial consequences not currently provided for in PIPEDA.
>
> New incentives, including changes to the enforcement model, are required to encourage organizations to be proactive, to build upfront protections, and to ensure secure treatment of individuals' personal information.[3] – Jennifer Stoddart, Former Privacy Commissioner of Canada

We also point you to the OPC's Position Paper on this issue, which concludes that "Canada cannot afford to be left behind, with little in the way of consequences for those that do not respect this country's federal privacy law."[4]

12. The sad reality is that the current enforcement system in PIPEDA is unequal to the task of protecting privacy in the digital age. Bill S-4 adopts a minimalistic and incremental approach to addressing this issue which might have been appropriate upon conclusion of PIPEDA's first 5 year review, in 2006, but is not enough at this stage of the digital era. We encourage the government to at minimum commit to fixing PIPEDA's regulatory regime in the near future.

13. Finally, the Bill's central privacy improvement – its attempt to impose a Breach Notification regime – falls short, and risks being ineffective at its important objectives, as described in response to the following question.

[2] https://www.priv.gc.ca/information/research-recherche/2010/pipeda_h_s_e.pdf
[3] http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=5938281&Language=E&Mode=1&Parl=41&Ses=1
[4] https://www.priv.gc.ca/parl/2013/pipeda_r_201305_e.pdf

Question 2: At our last meeting, the Canadian Chamber of Commerce and the Canadian Marketing Association both expressed concerns that the mandatory data breach reporting provisions contained in Bill S-4 would put an unnecessary burden on small businesses without providing addition protections to consumers. Do you think that mandatory data breach notifications will be an improvement in Canada's privacy regime?

14. Data breach notification obligations are rapidly becoming an international standard. They have been the norm in the United States for some time, with 47 out of 50 states having had such obligations in place for many years, and federal legislation now being introduced. The EU framework has also had an obligation in place for some time, soon to be formalized in a Directive. That Canada has not yet adopted such obligations is concerning. However, the regime proposed in Bill S-4, far from being too onerous on businesses (small or large), fails to go far enough.

15. In principle, breach notification addresses two essential problems. First, it allows customers affected by a data breach to take ameliorative measures to mitigate any resulting harm to credit, reputation or worse. Second, it provides an important incentive for companies to adopt reasonable technical safeguards. Both of these objectives are essential in an era where the prevalence of security threats is growing rapidly and where individuals are obligated to entrust increasing amounts of data to third parties as a condition of participation in the digital world.

16. Far from being onerous or heavy handed, the notification framework proposed by Bill S-4 does not go far enough. First, the framework it adopts for notification is problematic in that it fails to adequately ensure individuals will be notified of breaches that pose a real risk of significant harm to them. This is because it is left to organizations to decide when the notification threshold is reached or not. This is a problem with breach notification because companies consistently err on behalf of non-disclosure with respect to breaches that might, if reported, lead to reputational harm, short-term stock harm or the need to adopt costly technical solutions to properly address underlying issues. CIPPIC has witnessed this resistance first hand when working with companies in attempts to address discovered security breaches.

17. Bill S-4 attempts to mitigate this problem by obligating companies to keep internal records of *all* data breaches and providing the Privacy Commissioner the power to audit these lists to ensure that, on a historical basis, companies have properly applied the 'real risk of significant harm' notification standard. This recording obligation is an important one, but falls short in achieving its objective. First, by the time a history of mis-application is uncovered by the OPC through random

spot check audits, many individuals will have been robbed of their opportunity to mitigate the risk of harm imposed on them by historical breaches. Second, relying on spot audits will not provide the OPC with a comprehensive picture of industry practices, hindering its ability to issues guidelines that could assist in securing meaningful compliance. Third, Clause 26 of Bill S-4 imposes strict gag provisions onto the OPC regarding any information it obtains from these spot-audits, further hindering its ability to issue general guidelines and limiting any incentive to 'get it right' by mitigating the prospect of reputational damages. Finally, the OPC cannot impose any binding orders onto those demonstrating a history of standard mis-application.

18. In this regard, Bill S-4 offers some improvements over its predecessor. Specifically, the federal court trial *de novo* remedies have been expanded to include fines for knowing breaches and the ability to "order an organization to correct its practices in order to comply with" data breach notification obligations. However, the fines in question require a high standard of intent, meaning they will rarely if ever be implicated. Indeed, the fining mechanism used was designed for willful obstruction of justice and destruction of evidence. It is ill-suited for regulating compliance with a data breach notification regime. Moreover, Division 1.1 does not grant individuals access to the record-keeping databases held by companies, making any individually-driven complaint an unlikely prospect.

19. Bill S-4 is also deficient with respect to its ability to meet the second objective of breach notification regimes, which is target hardening. The single most effective step the government can take in order to improve the security of our networks is to put in place proper incentives for organizations to effectively secure data.[5] As policy-makers have noted, effective breach notification is becoming a centrally important tool for measuring the overall performance of security safeguards in addressing the increasing challenges inherent in securing data:

> Notice helps consumers protect themselves against harms such as identity theft. It also provides companies with incentives to establish better data security in the first place. The [breach notification] model is also gaining acceptance internationally as a performance-based requirement that effectively protects consumers.[6]

However, Bill S-4 only requires notification of breaches that raise a real risk of significant harm to individual users. This is a high standard –higher than the standards of corresponding regimes

[5] See: https://www.accessnow.org/blog/2014/12/23/sony-pictures-hack-shows-weak-security-but-no-reason-to-violate-privacy-sta for one example.
[6] https://www.whitehouse.gov/sites/default/files/privacy-final.pdf

in the United States (proposed: breach poses "no reasonable risk of harm or fraud")[7] and European Union (breach "likely to adversely affect the personal data or privacy of a data subject").[8] In addition, the EU framework requires the reporting of "all personal data breaches" to national privacy commissioners. In this regard, too, the reporting obligations in Bill S-4 are far less onerous than those proposed by other countries.

20. While the rigidness of Bill S-4's reporting standard is mitigated to some degree by its inclusive definition of 'harm', the result of its approach is nonetheless that a much smaller subset of breaches will be captured by the regime, leaving many material breaches unreported. However, the reality of technical safeguards is that many breaches are indicative of specific laxities in technical safeguard obligations, even where they do not directly threaten substantial harm to specific individuals. The current scheme of Bill S-4 would require these breaches to be recorded, but not reported, meaning that they will not come to the attention of the public or of the Office of the Privacy Commissioner. It has been CIPPIC's experience that, all too often, companies faced with broken safeguards will adopt ineffective and less costly quick fixes in lieu of the robust solutions necessary to definitively address underlying problems. It is therefore important to ensure that all material breaches are brought to the attention of the Privacy Commissioner, so that there can be tracking and objective oversight to ensure that companies are taking reasonable steps to secure customer data, as required by law.

21. We realize that the high and under-inclusive standard by Bill S-4 ('real risk of significant harm') mirrors that adopted in Alberta. While the Alberta framework provides for a more active role to be played by the Information and Privacy Commissioner in determining when this standard is engaged, we do not view the Alberta regime as an effective means of achieving either of the stated objectives of breach notification, as it only applies to a small subset of relevant breaches. This is particularly so with respect to safeguard breaches in federally regulated contexts such as banking and telecommunications. The European approach which has been in place since 2013 is the most effective means of placing proper incentives to secure our networks. It requires reporting of most data breaches to national privacy authorities. However, an acceptable alternative, a modification of the proposal in Bill S-4's predecessor, Bill C-12,

[7] https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf
[8] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

which would have obligated companies to report any *material* breach, defined (with slight modification) as follows:

RECOMMENDATION

10.1 (1) An organization shall report to the Commissioner any material breach of security safeguards involving personal information under its control.

(2) The factors that are relevant to determining whether a breach of security safeguards is material include

(a) the sensitivity of the personal information; and

(b) the number of individuals whose personal information was involved~~; and~~.

~~(c) an assessment by the organization that the cause of the breach or a pattern of breaches indicates a systemic problem.~~

The cause of a breach should be deemed material if it indicates a systemic or recurring problem.

The modification above is designed to ensure that organizations cannot avoid reporting of serious breaches simply because they are not (or no longer) indicative of a systemic problem. This will ensure all meaningful breaches are captured in some manner (the specific reporting obligations can be refined by regulation, and need not be expansive).

Question 3: How does the Supreme Court decision in R. v. Spencer affect this bill?

22. It's useful to include some background on *R. v. Spencer* as context for this answer. The Supreme Court of Canada's decision in *R. v. Spencer* addressed the parameters under which companies can voluntarily share customer information with a state investigative agency. It additionally recognized the important privacy interest inherent in online identifiers held by third parties such as ISPs. This identity information was designated as 'not very private' by ISPs many years ago and, further to that designation, ISPs have voluntarily identified millions of anonymous Canadians to state agencies ever since (over 700,000 Canadians were identified in 2011 alone). This invasive program of *en masse* voluntary identification occurred under the auspices of paragraph 7(3)(c.1) of PIPEDA, which allows private parties to share customer information with state agencies identifying their 'lawful authority'.

23. Bill S-4 ignores the lessons of Spencer in three ways. First, it expands the conditions under which we will be relying on organizations such as ISPs to assess the law when policy-level decisions are made regarding the private information of their customers. ISPs and other companies are not courts. They lack the capacity, expertise and legitimacy to properly assess whether the legal claim of a third party – be it a law enforcement agency or a private litigant – is sufficiently accurate to justify access to customer information. In 2008, Canadian ISPs collectively decided that there is no reasonable expectation of privacy in online anonymity. The Supreme Court's decision in *Spencer* finally and definitively determined that this was wrong. However, in the interim, the program invaded the privacy of millions of Canadians in their anonymous online activities over the years. Aside from a few instances where this violation led to direct criminal charges, these millions of affected Canadians had no opportunity to challenge their ISPs' decision. The investigative exception proposed by Bill S-4 once again relies heavily on organizations to decide when it is or is not appropriate to disclose customer information of their customers in order to achieve broader policy objectives (third party litigation/investigations) that they are ill-suited to weighing.

24. Second, the *Spencer* decision provided important context and insight into the privacy implications of identity disclosure by Canadian ISPs. Yet ambiguities remain regarding its application to a number of other contexts that are ill-studied and similarly obscured. Can banks hand over customer information under current paragraph 7(3)(c.1)? Can intelligence agencies request identification information from ISPs? From Email providers? These contexts are similar, but some may argue that a different set of privacy expectations are engaged, leading to potentially different interpretations. By leaving paragraph 7(3)(c.1) intact, Bill S-4 leaves the resolutions of these ambiguities to organizations, replicating the problems identified in *Spencer* on an ongoing basis. Bill S-4 is a significant improvement over its predecessor, Bill C-12, in this regard as it removes a clause that would have purported to extend the application of paragraph 7(3)(c.1) to warrantless disclosures. However, in the 2004 consultations that led to Bill S-4, CIPPIC called for the repeal of paragraph 7(3)(c.1). We continue to view it as problematic, all the more so in the wake of *Spencer*.

25. Finally, by failing to legislate much needed transparency obligations onto companies, Bill S-4 misses an important opportunity to ensure the systemic problems exposed by *Spencer* are not repeated. In this regard, Bill S-4 does not clarify that PIPEDA's openness principle requires annual transparency reporting of lawful disclosures and requests by at least some companies,

such as ISPs and Banks. Secondly, while Bill S-4 improves on its predecessor (Bill C-12) by removing gagging provisions that would have effectively prevented organizations from notifying customers their data has been requested or disclosed, it fails to impose positive individual notice obligations. It is our view that the lack of such an individual obligation threatens the constitutionality of PIPEDA. Adding transparency reporting and individual notice obligations is also good policy. It will help identify problematic disclosure practices such as the one addressed in *Spencer* within a reasonable time frame, so that these can be directly and immediately challenged by affected individuals.

CONCLUSION

26. We wanted to once again thank the NDP members of the Committee for providing us this opportunity to expand on our views of Bill S-4, and to thank all Committee members for their careful attention to this Bill. It is an important one, but in our view one that still requires some work to meaningfully further the protection of privacy in the digital age.

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