May 30, 2014

VIA EMAIL

The Right Honourable Stephen Harper
Prime Minister of Canada
House of Commons
Ottawa, ON, KIA 0A6
stephen.harper@parl.gc.ca

To the Right Honourable Prime Minister Steven Harper

Re: Canada's Growing Privacy Deficit

We write you to express our grave concern regarding Canada's growing privacy deficit, evident in a number of the government's policies and practices, including its refusal to fix privacy-invasive elements of Bill C-13, its failure to address long-standing and well documented privacy problems and its nomination of a Privacy Commissioner of Canada who lacks the immediate expertise to tackle Canada's long list of privacy challenges.

Bill C-13, the *Protecting Canadians from Online Crime Act*, is not receiving the full and robust consideration its privacy-threatening elements deserve before the Standing House of Commons Committee on Justice and Human Rights. Specifically, we join Ontario Information & Privacy Commissioner Ann Cavoukian, B.C. Information & Privacy Commissioner Elizabeth Denham, the Canadian Bar Association, and a number of other experts and affected individuals in calling for the severance of the cyber-bullying-specific elements of this Bill from the lawful access portions of the Bill. The merger of these two issues in one bill has been a direct impediment to any meaningful debate of the issues arising from these two quite distinct initiatives. Additionally, we wish to express a more general concern over this government's growing disregard for the privacy of Canadians. The government has been quick to repeatedly update police investigative powers in order to meet the challenges of the digital age (this is, in fact, the lawful access component of Bill C-13), but has refused to fix long-standing and well acknowledged privacy problems arising from the same technological developments. This general disregard for the need to update privacy protections is exacerbated by the government's recent nomination of a Privacy Commissioner of Canada who lacks the immediate expertise and perspective necessary to tackle Canada's many pressing privacy challenges.

Bill C-13: Lack of Meaningful Debate Will Lead to Serious Privacy Violations

While many of the new investigative powers proposed in Bill C-13 are acceptable, a number of them represent a serious over-reach. These include particularly (but not exclusively):

- **Categorical immunity for voluntary data-sharing schemes:** Currently, telecommunications and other companies may voluntarily provide or preserve customer data upon request, but must act reasonably and in good faith when responding to requests for doing so. Bill C-13 will remove the existing obligation to act reasonably and in good faith;

- **Expanded Definition of Public Officers:** Bill C-13 will expand the definition of 'public officers' to include any individual tasked with administering or enforcing a law of Canada or a province. This will let a long list of entities, including the Communications Security Establishment, the Canadian Security Intelligence Service and the Canada Revenue Agency, to use a range of *Criminal Code* powers as well as to rely on immunities granted for voluntary sharing;

- **Transmission Data Available on Reasonable Suspicion:** Transmission data is metadata which includes at minimum: telephone numbers called or texted, duration of calls, origin and destination IP addresses, websites visited, type of application being used, type of Internet communication (VoIP, Email, mobile application) and unique mobile device identifiers. It can also include URLs of webpages visited, search queries and email subject lines. This information is as sensitive as the content of our emails, phone calls and text messages (if not more so), yet Bill C-13 will let state agents access it upon a mere reasonable suspicion that the privacy invasion will assist an investigation of an offence – a broad investigative power typically reserved for the least sensitive of information;

- **Tracking Data Available on Reasonable Suspicion:** Tracking data refers to the detailed location information that is constantly generated by the mobile phones, cars and wearable computing devices that are becoming a ubiquitous feature of our society. Technological and social developments have made it possible to obtain the rich and detailed location information generated by these devices from a range of third parties including telecommunications companies, mobile device manufacturers, social networking sites and insurance companies. Bill C-13 will let state agents access this information upon a mere reasonable suspicion that the privacy invasion will assist an investigation of an offence – a broad investigative power typically reserved for the least sensitive of information.

Collectively, these and other problematic elements of Bill C-13 will dramatically expand the state's capacity to invade the privacy of Canadians.

Bill C-13's merger of two distinct issues (cyber-bullying and new law enforcement powers) is impeding meaningful debate of these matters. On the one hand, this merger has impeded a necessary and complete debate of the problem of cyber-bullying, a broad-ranging social problem that will likely not be solved by the addition of a single *Criminal Code* provision. On the other hand, the focus on cyber-bullying has impeded meaningful discussion of the lawful access components of Bill C-13. The new investigative powers proposed in Bill C-13 are powers of general application and will only rarely be employed in the context of cyber-bullying. However, given the understandably important and immediate concerns raised by the problems of cyber-bullying, the discussion of lawful access powers before this committee has been focused predominantly around that one use-case, leading to an incomplete view of how these new powers will impact disproportionately on the privacy of Canadians.

In fact, fixing the problematic investigative powers will not impede investigations of cyber-bullying matters. Cyber-bullying matters typically follow particular patterns. They will involve an individual who is being harassed by means of digital networks. The harassing comments, improper images or threatening/defamatory content that forms the basis of a cyber-bullying offence will typically be sent or published anonymously. As the cyber-bullying crime at issue in digital environments relates primarily to the posting or sending of such content, police will have the reasonable belief necessary to obtain any production order or warrant they wish. They will have facial evidence of the offence – be it child pornography, extortion, threatening, harassment or the proposed section 162.1 offence – which is all that is required to meet the higher standards for transmission and tracking data that we and others have called for.

Moreover, telecommunications companies in Canada regularly share immense amounts of customer data with law enforcement voluntarily and outside of any legal authorization. This system of information sharing has developed under the current *Criminal Code* immunities for voluntary sharing. In light of this existing robust system of information-sharing, there is little justification or need for removing the current obligation for companies to act reasonably and in good faith when responding to extra-legal government requests. Replacing these with categorical immunity from any civil or criminal liability removes any incentives companies might have to approach the decision to give away sensitive customer information with a degree of caution. No other exceptional power is needed to investigate typical cyber bullying offences.

The significant and novel nature of the issues contained in Bill C-13 – issues that have never before been examined in legislative committee – has also led to key stakeholders being excluded from the discussion. With respect to lawful access, a number of civil liberties and digital rights groups have developed significant expertise over the years on the subject matter of this Bill, and can point to a long history of engagement on this specific legislative package. In addition, Canada's federal and provincial Privacy Commissioners have significant expertise on this subject matter. However, the attempt to address cyber-bullying and lawful access matters in one set of committee hearings has led to the exclusion of many of these groups in order to accommodate a long list of experts and affected parties on *both* issues. Notably, not one civil liberties or privacy group has been invited to testify, and not one Privacy Commissioner will have the opportunity to do so. Moreover, we note that while some sessions of this committee study have focused exclusively on cyber-bullying, the lawful access elements of the legislation have not received the same level of dedicated consideration, contributing to the predominant examination of Bill C-13's investigative powers through the narrow context of cyber-bullying investigations.

We therefore call on the government, through its majority control of the Standing House of Commons Committee which is currently reviewing this legislation, to bifurcate Bill C-13 so that meaningful discussion of its distinct cyber-bullying and lawful access components can be discussed in isolation.

Growing List of Privacy Problems Left Un-Addressed

The problems arising from Bill C-13 and the failure of a meaningful discussion of its privacy shortcomings in Committee are indicative of a broader disregard that is becoming evident in this government's approach to privacy. The lawful access components of Bill C-13 are designed to update police powers for the 21st century. However, law enforcement powers have been updated many times to meet the technical challenges of the digital age. Indeed, many of the powers that are supplemented and amended by Bill C-13, including the general production power and the general immunity for voluntary third party cooperation with police investigations (current

sections 487.012 and 487.014 of the *Criminal Code*, respectively), were introduced as recently as 2004.[1]

This constant and sustained effort to update police powers in order to meet technical challenges has been matched with a failure to similarly update privacy protections by its refusal to address long-standing privacy problems. These include:

- Failure to address or acknowledge serious and well documented problems arising from shortcomings in the oversight, accountability and authorization regime for Canada's foreign intelligence agency, the Communications Security Establishment of Canada;

- Failure to address or critically examine state surveillance in Canada. While the wiretapping provisions of the *Criminal Code* include comprehensive statistical reporting and individual notice obligations, there is no comparable transparency requirement regarding any other state surveillance practices. Exacerbating this transparency problem is the significant degree of state access to data that relies on voluntary cooperation of private companies and, hence, occurs outside of any legal authorization regime. While these companies are permitted by law to facilitate state investigations, they are prevented by law from informing the public of the scope of such disclosures through existing legal instruments;[2]

---

[1] Debates of the Senate, 3rd Session, 37th Parliament, Volume 141, Issue 11, February 18, 2004, discussing Bill C-13, *an Act to amend the Criminal Code (capital markets fraud and evidence-gathering)*, Honourable Senator Wilfred P. Moore, <http://www.parl.gc.ca/Content/Sen/Chamber/373/Debates/011db_2004-02-18-e.htm?Language=E>:
"The third element of Bill C-13 is the creation of enhanced evidence-gathering tools. In response to the legitimate needs of front-line investigators, Bill C-13 will create two types of "production order" powers in the Criminal Code. These production orders are for the most part based on similar standards and safeguards as search warrants... Honourable senators, it is important to note that these new production orders will be available in general to the investigation of all criminal offences... Law enforcement agencies and Crown prosecutors have been asking for this new legislative tool for some time. With the increasing computerization of records, the proliferation of the Internet and the widespread adoption of new communications technologies, the timing is right for this form of investigative tool.

[2] In response to requests spearheaded by the Citizen Lab, a number of Canadian telecommunications companies have refused to disclose even aggregate numbers regarding the frequency and character of law enforcement requests they receive, citing concerns over legal liability: C. Parsons, "The Murky State of Canadian Telecommunications Surveillance", March 6, 2014, CitizenLab.org, <https://citizenlab.org/2014/03/murky-state-canadian-telecommunications-surveillance/>. See also Standard 17 of the Solicitor General Enforcement Standards (SGES), which imposes the following obligation onto wireless telecommunications companies: "Law enforcement agencies require network operators/ service providers to protect information on which and how many interceptions are being or have been performed, and not disclose information on how interceptions are carried out." Solicitor General Enforcement Standards for Lawful Interception of Telecommunications – Compliance Table, Current as of November 17, 2008, <https://cippic.ca/uploads/Solicitor_General_Standards_Annotaed-2008.pdf>, imposed on providers of wireless services as a condition of spectrum license: Industry Canada, Licensing Framework for Mobile Broadband Services (MBS) – 700 MHz Band, march 7, 2013, <http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf10581.html>, paras. 291-292.

- Failure to conduct a mandatory statutory review of PIPEDA, Canada's federal privacy protective framework. This review was statutorily mandated to have occurred in 2011. The inclusion of minor additional reforms in Bill S-4 does not address the range of long-standing privacy problems that must be addressed in order to keep PIPEDA relevant;[3]

- The government has refused to update two additional statutes essential to effective privacy protection and transparency in surveillance: the *Privacy Act*, which has not been meaningfully reformed since it was first enacted over 30 years ago,[4] and the *Access to Information Act*, which was enacted in 1982, has not been updated for the digital age and lacks key obligations such as a duty to document.[5]

This ongoing neglect is troubling. We call on the government to establish a panel or royal commission to examine state surveillance and privacy protection in the digital age.

Canada's Next Privacy Commissioner

With great respect and without any intended slight on his abilities, we feel obligated to object to the Government's recently announced appointee for Privacy Commissioner of Canada, Mr. Daniel Therrien. As long-standing Assistant Deputy Attorney General for Public Safety, Mr. Therrien lacks the perspective and experience necessary to immediately tackle Canada's many privacy problems. Privacy protection – and particularly commercial privacy as protected by the *Personal Information Protection and Electronic Documents Act* (PIPEDA) – is a highly specialized field, with greatly nuanced legal and policy challenges. The Assistant Deputy Attorney General for

---

[3] See: M. Geist, "What Happened to PIPEDA Review", December 16, 2011, <http://www.michaelgeist.ca/content/view/6208/125/>; Office of the Privacy Commissioner of Canada, "The Case for Reforming the *Personal Information Protection and Electronic Documents Act*, May 2013, <https://www.priv.gc.ca/parl/2013/pipeda_r_201305_e.pdf>; Report of the Standing Committee on Access to Information, Privacy & Ethics (ETHI), "Privacy and Social Media in the Age of Big Data", April 2013, <http://www.parl.gc.ca/content/hoc/Committee/411/ETHI/Reports/RP6094136/ethirp05/ethirp05-e.pdf>.

[4] See: Honourable Rob Nicholson, Minister of Justice, Government Response to Recommendations of the Standing Committee on Access to Information, Ethics & Privacy on the Need to Update the Privacy Act, 2009, <http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=4139208&Language=E&Mode=1&Parl=40&Ses=2>; Jennifer Stoddart, Privacy Commissioner of Canada, "The Necessary Rebirth of the *Privacy Act*", November 29, 2013, <http://www.priv.gc.ca/media/sp-d/2013/sp-d_20131129_02_e.asp>.

[5] See: Honourable Rob Nicholson, Minister of Justice, Government Response to Recommendations of the Standing Committee on Access to Information, Ethics & Privacy on the Need to Update the Access to Information Act, 2009, <http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=4139070&Language=E&Mode=1&Parl=40&Ses=2>; Suzanne Legault, Information Commissioner of Canada, Speaking Notes to the Canadian Legal Information Institute (CanLII) Conference, September 13, 2013, <http://www.oic-ci.gc.ca/eng/media-room-salle-media_speeches-discours_2013_5.aspx>.

Public Safety is accustomed to approaching privacy issues from a wholly opposite perspective that does not engage these specific nuances. Moreover, Mr. Therrien's direct responsibility for and oversight of many of the programs that he will now be called upon to advocate against will exacerbate the already steep learning curve with which he is faced. We are further concerned that, in light of his role as legal adviser on a number of these programs, Mr. Therrien may face conflicts of interest that could effectively disqualify him from challenging these programs as Privacy Commissioner. The lack of a strong privacy watchdog, particularly at this juncture when critical issues are being decided that will impact the privacy of Canadians for decades to come, is indefensible.

We therefore respectfully urge the government to reconsider its nomination of Mr. Therrien as Privacy Commissioner of Canada.

Conclusion

In conclusion, we hope that this letter will remind the government of its obligation to safeguard the privacy of Canadians. We would be pleased to engage with the government on any of these or related issues.

SIGNATORIES