August 9, 2011

VIA EMAIL

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

Dear Prime Minister Harper,

RE: Omnibus Crime bill

We are writing to you regarding your promise to introduce and pass within 100 days an omnibus bill incorporating a number of very different pieces of legislation.

We are particularly concerned that three of those bills will have serious negative implications for the privacy rights of Canadians, and that these aspects will not receive the scrutiny they deserve if rolled into an omnibus bill.

These pieces of legislation were former Bills C-50, C-51 and C-52 from the last session of the previous Parliament, the 'lawful access' technical surveillance bills. We join Canada's federal and provincial Privacy Commissioners in voicing our grave concerns regarding this invasive legislative mandate, as they collectively did in a letter to Deputy Minister of Public Safety dated March 9, 2011. Our specific concerns, which we highlight in greater detail in an appendix to this letter, include:

- The ease by which Canadians' Internet service providers, social networks, and even their handsets and cars will be turned into tools to spy on their activities further to production and preservation orders in former Bill C-51 – a form of spying that is bound to have serious chilling effects on online activity and communications, implicating fundamental rights and freedoms;
- The minimal and inadequate amount of external oversight in place to ensure that the powers allotted in these bills are not abused;
- Clause 16 of former Bill C-52, which will allow law enforcement to force identification of anonymous online Internet users, even where there is no reason to suspect the information will be useful to any investigation and without adequate court oversight; and
- The manner in which former Bill C-52 paves the way to categorical secrecy orders that will further obscure how the sweeping powers granted in it are used and that are reminiscent of elements of the USA PATRIOT Act that were found unconstitutional.

On a final note, we object that Canadians will be asked to foot the bill for all this, in what essentially amounts to a hidden e-surveillance tax, and are concerned that compliance will further impede the ability of smaller telecommunications service providers to compete in Canada by saddling them with disproportionate costs.

The implications of all of this demand careful scrutiny and study. Yet none of these bills has had the benefit of hearings before any Parliamentary committee, nor have any of their numerous predecessor bills, introduced by both your government and the previous Liberal government.

Your government has already recognized the divisibility of this proposed omnibus bill by passing Bill C-2, dealing with large criminal trials, which was once proposed to be part of the omnibus bill.

Given the profound concerns raised by Canada's Privacy Commissioners which have yet to be answered, we ask you to at least give these pieces of legislation an appropriate hearing. That cannot happen if they are rolled into an omnibus crime bill with a large number of unrelated and also contentious pieces of legislation.

We look forward to your response, and are more than willing to provide you with any additional information you or your government may require in this regard.

cc: Hon. Vic Toews, Minister of Public Safety, vic.toews@parl.gc.ca
Hon. Rob Nicholson, Minister of Justice, rob.nicholson@parl.gc.ca

Signed by the following individuals and organizations:

Andrea Slane, University of Ontario Institute of Technology, Faculty of Social Science & Humanities
Andrew Clement, University of Toronto, Faculty of Information
British Columbia Freedom of Information and Privacy Association (BCFIPA)
Canadian Association of University Teachers (CAUT)
Canadian Civil Liberties Association (CCLA)
Canadian Federation of Students (CFS)
Christopher Parsons, University of Victoria, Department of Political Science
Civil Liberties Association – National Capitol Region (CLA–NCR)
Colin Bennett, University of Victoria, Department of Political Science
David Lyon, FRSC, Queen's University, Surveillance Studies Centre
Ian Kerr, University of Ottawa, Faculty of Law
International Civil Liberties Monitoring Group (ICLMG)
Kate Milberry, University of Toronto, Faculty of Information
Leslie Shade, Concordia University, Department of Communications Studies
Lisa Austin, University of Toronto, Faculty of Law
Michael Geist, University of Ottawa, Faculty of Law
Michael Markwick, Simon Fraser University, School of Communications
OpenMedia.ca
Public Interest Advocacy Centre (PIAC)
Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)
Sharon Polsky, President, AMINACorp.ca; National Chair, Canadian Association of Professional Access & Privacy Administrators (CAPAPA)
Teresa Scassa, University of Ottawa, Faculty of Law
Valerie Steeves, University of Ottawa, Department of Criminology

APPENDIX A

For convenience, we include here a more detailed elaboration of our concerns and the basis thereof.

<u>Turning Canadians' Networked Services Against Them</u>:

First, we are concerned that a broad range of preservation and production orders put in place in former Bill C-51 are calculated to turn Canadians' Internet service providers and other Internet intermediaries, their social networking sites, and even their very handsets and cars, into tools to better spy on their activities. Highly contentious are orders aimed at discovering the location of objects such as cellular phones or GPS devices or of transactions such as geo-tagged comments or photos from private sector service providers contained in former Bill C-51.[1] This information of Canadians who have not done anything wrong will be available to law enforcement as long as there is a reason to suspect it will be generally 'useful' to an investigation. Equally troubling are preservation demands that can force online organizations to store vast amounts of customer information upon request, without any prior judicial approval or oversight, wherever a police officer suspects the data might be helpful to an investigation. Given the ever-increasing amount of information on Canadians that is electronically accessible, *stronger* standards of protection are required, not weaker ones.

Finally, we are concerned with the legitimizing effect these orders will have on voluntary public-private cooperation, generally. Such cooperation turns private organizations against their customers and can undermine civil liberties as it occurs outside of safeguards existing within the *Charter of Rights and Freedoms*, which does not apply to private action. The legitimate role of Canada's private sector is to provide services to customers, not to act as state agents with a mandate to spy on online activity. This legitimizing effect is complicated by murky liability immunization provisions for voluntary cooperation such as that found in former Bill C-51.[2]

<u>Inadequate External Oversight</u>:

Second, external oversight mechanisms to track the extent to which searches and seizures of sensitive personal information under these sweeping new powers are conducted in an abusive manner are, at best, illusory. Former Bill C-52, for example, places *obligations* on Canada's Privacy Commissioners to ensure the new powers it grants are not abused, but it fails to provide the Commissioners with any of the tools and resources that are a pre-requisite to effective oversight. For example, Clause 20(4) mandates Canada's Privacy Commissioners to use existing audit powers in order to monitor RCMP compliance. No new powers and no new resources are granted. Further, with respect to Provincial and municipal police, no auditing mandate is put in place at all. Indeed, many provincial Privacy Commissioners lack the statutory authority necessary to perform even the rudimentary audits envisioned federally by Clause 20(4). This appears to be a serious lapse, as municipal and Provincial police are expected to make most heavy use of new powers awarded in former Bill C-52.

---

[1] Clause 13 of former Bill C-51, which would have amended the *Criminal Code* by adding section 487.017.

[2] Clause 13 of former Bill C-51, which would have replaced existing section 487.014(2) of the *Criminal Code* with proposed section 487.0195(2).

The intrusive powers proposed by former Bills C-51 and C-52 require far stronger external oversight to track abuse. Comparisons with oversight regimes overseen by data protection authorities in other jurisdictions demonstrate with clarity the woeful inadequacy of oversight as envisioned in the lawful access legislation. These international examples also demonstrate that it is not difficult to put in place workable oversight regimes that do nothing to impede the ability of law enforcement to conduct their legitimate duties. Yet the latest iteration of the lawful access legislation makes no attempt to enact such a regime. Indeed, former Bill C-52 puts in place far more expansive and rigorous oversight to ensure private sector compliance with its intrusive requirements than it does to ensure lack of police abuse.

Identifying Canadians Online:

Third, we turn to the warrantless powers included in Clause 16 of former Bill C-52 that will permit law enforcement to seize 'subscriber data' from telecommunications service providers. Access to subscriber data, as defined in the proposed legislation, raises serious privacy implications. It includes data that will allow state agents to identify anonymous online individuals at their sole discretion. Anonymous activity is integral to online speech and expression and is a key mechanism for ensuring privacy in a world where the list of individual activities that occur (and are recorded) online expands almost daily.

We believe that the surveillance capacities enabled by the many identifiers included in Clause 16 have been underestimated. IP addresses and email accounts, for example, can be used to track anonymous user activity across numerous websites and services and, with Clause 16 powers, to connect this information to a real-life identity. The tracking enabled by persistent device identifiers such as those included in Clause 16 is not well understood, as the Information & Privacy Commissioner of Ontario recently pointed out with respect to WiFi device identifiers.

Clause 16 will give state agents the power to access all of this highly sensitive personal information, even where there is no reason to suspect it will assist in the investigation of any offence. Indeed, former Bill C-51[3] will already grant state agents access to such data in any scenario where there *is* reason to suspect the information could assist in an investigation – a bar that is quite low to begin with. Yet Clause 16 goes further. What Clause 16 facilitates, simply put, are unjustified and seemingly limitless fishing expeditions for private information of innocent and non-suspicious Canadians.

Paving the Way to Sweeping Secrecy Orders:

Further compounding the transparency and oversight problems already inherent in former Bill C-52 are two provisions that pave the way to sweeping gag orders that will prevent individuals from effectively challenging abuses of the powers granted therein. Clause 6(2) permits the government to impose, in regulations, sweeping and categorical confidentiality obligations on service providers that will apply across all interception warrants. Second, under Clause 71, any telecommunications service provider obligated to comply with a warrantless seizure request

[3] Clause 13 of former Bill C-51, which would have amended the *Criminal Code* by adding sections 487.013 and 487.015.

will be subject to the secrecy provisions in proposed section 7.4 of PIPEDA. Proposed section 7.4 of PIPEDA prevents organizations from disclosing the fact of their cooperation with state efforts to spy on their customers. The sweeping nature of the secrecy measures envisioned by these provisions is in stark contrast to existing practice, where gag orders must be requested from a judge and justified on a case by case basis. The problem with such measures is that they will prevent individuals from challenging abuses of the powers granted in this Bill. Indeed, with categorical secrecy orders in place, surveillance that overreaches is least likely to ever be challenged in court, as the results of such surveillance are less likely to later appear in Court proceedings.