Information & Privacy Commissioner
Ontario, Canada

Commissaire à l'information et
à la protection de la vie privée
Ontario, Canada

Leading the Way – Positive-Sum Solutions to Protecting Privacy, Civil Liberties and Security

Submission to the U.S. Privacy and Civil Liberties Oversight Board by the Information and Privacy Commissioner, Ontario, Canada

October 2013

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
M4W 1A8

416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9195
TTY: 416-325-7539
Website: www.ipc.on.ca

Leading the Way – Positive-Sum Solutions to Protecting Privacy, Civil Liberties and Security

Submission to the U.S. Privacy and Civil Liberties Oversight Board by the Information and Privacy Commissioner, Ontario, Canada

Table of Contents

1. Introduction

On September, 23, 2013, David Medine, the Chair of the United States Privacy and Civil Liberties Oversight Board (PCLOB), invited privacy commissioners assembled at the 35th International Conference of Data Protection and Privacy Commissioners in Warsaw, Poland, to make submissions to the PCLOB in the context of its upcoming hearings on the U.S. government's counter-terrorism surveillance programs.

These hearings were announced shortly after Edward Snowden had disclosed a classified court order that revealed a top secret and sweeping National Security Agency (NSA) metadata surveillance program. Since then, the public has been presented with a steady stream of revelations about the range, scope, and scale of the domestic and foreign intelligence gathering activities of the NSA and its *Five Eyes* allies. Further reverberations are expected as citizens, elected officials, governments and corporations around the world continue to grapple with the implications for privacy, human rights, freedom, democracy, Internet governance, Internet commerce, international relations, and national security.

In this context, and in direct response to Chairman Medine's invitation, the Information and Privacy Commissioner of Ontario, Canada, has prepared the following written submission. We offer this submission in furtherance of the goal of developing recommendations for changes to these programs and the operations of the Foreign Intelligence Surveillance Court (FISC) to ensure that counter-terrorism efforts protect privacy and civil liberties.

2. Challenges and Opportunities

In our view, a unique opportunity exists to develop a new approach to facilitating *necessary* national security intelligence gathering while simultaneously ensuring privacy and freedom for all citizens. The challenge is to design legal and technological systems that protect both privacy and national security in a global context, shaped by national self-interest, but also by increasing economic, social, and technical interdependence.

We realize this is no minor challenge. Terrorism is but one of many complex issues caught up under the national security rubric. Terrorist attacks, however infrequent in North America, come with heavy economic, political, and human costs. At the same time, there are high costs associated with disproportionate or ill thought out national security programs. Beyond the billions of dollars spent on secretive programs and facilities, there are collateral costs. Simply consider that efforts to weaken encryption standards, as well as to co-opt communications service providers into creating secret security gaps or back doors in communications systems, not only threaten an open and secure Internet, but they have also set a chill to work at the heart of the North American Internet economy. Whatever the final figures, estimates of lost opportunities over the coming years are in the hundreds of billions of dollars.

No less importantly, people of every political stripe know that governments that have not been truthful about the size, scope, or purpose of their security programs run the risk of undermining citizen trust in one's government. This is currently manifesting itself in the growing distrust of government that exists today.

To the outrage of many citizens and elected leaders, it is now clear that post-9/11, foreign and domestic intelligence surveillance programs have been designed to be both sweeping in their scope and opaque in their technical and legal operations. Classified rules designed to limit the collection and use of communications have been breached. Congressional and judicial bodies tasked with providing 'in camera' oversight have been caught off guard. Top security officials have been forced to admit that they have frequently misinformed the judiciary, Congress, and the public about the handling of citizens' data, as well as having exaggerated the role of sweeping surveillance in preventing domestic terrorism. Meanwhile, the only officials with complete and unfettered access to the facts – the security chiefs themselves – continue to offer the public blanket assurances that their sweeping powers are necessary and lawful, that no significant abuses have taken place, and that only cosmetic changes to the current system are required – to the disbelief of the public.

With no disrespect intended to the officials tasked with ensuring public safety, we submit that these assurances are fundamentally insufficient. Free societies must, of course, be protected from terrorism and genuine security threats today, but they must also be protected from the threat of tyranny tomorrow. Both threats must be addressed in the design of national security programs and the countervailing oversight required.

At the same time, in proposing a dynamic, solutions-oriented approach, we urge cautious optimism. Despite the disturbing aspects of so many of the revelations, no one should doubt that the United States has a leadership role to play. In fact, as America starts to shake off the common, nearly absolutist approach to secrecy in this area, a new approach may become possible, not only for the United States and its *Five Eyes* allies, but for democracies around the world.

However, given the implications for privacy and freedom, it is critical that, going forward, we challenge the widespread "either/or," "zero-sum" mindset of privacy **vs.** security. Under this increasingly dated approach, it is assumed that the goal of achieving security means that privacy must be sacrificed. We reject the view that in order to have security, we must give up privacy. We do not. Instead, we believe that what is needed are doubly-enabling, positive-sum measures designed to provide for both security **and** privacy, in an accountable and transparent manner.

3. Positive-Sum Solutions

Together, domestic and foreign intelligence agencies look outward and inward; out at other countries' citizens, and in at their own. In many countries, they do so with even less oversight than that provided for under American law. If we are to protect our own rights and liberties here in North America, then we must work to protect our rights and liberties globally. This is consistent with our shared hope that freedom will grow in every country, for all citizens.

Accordingly, we assert that where complex and sweeping domestic or foreign surveillance programs can be justified, they require matching, in-depth, sophisticated safeguards. The solution is to prioritize a system of dynamic symmetrical oversight, based on transparency in lawmaking, effective mechanisms to ensure accountability, and new technological measures such as a system of *Privacy-Protective Surveillance*. In our view, this three-part approach will be capable of protecting national security at "home," while securing our rights to a private life, free from unreasonable interference by the state.

A. Privacy-Protective Surveillance

Privacy-Protective Surveillance (*PPS*) is a positive-sum alternative to current counter-terrorism surveillance systems. The Information and Privacy Commissioner of Ontario, Canada, developed this concept with Professor Khaled El Emam, of the University of Ottawa. The attached paper, *Introducing Privacy-Protective Surveillance: Achieving Privacy and Effective Counter-Terrorism*, explains the concept in significantly greater detail.

The essential premise underlying *PPS* is that necessary national security-driven surveillance can be both effective and privacy-protective. Could *PPS* be applied to programs such as telephone metadata or foreign "private communications" surveillance programs? While *PPS* is still at a conceptual stage, we believe the answer is an emphatic "yes." Efforts are already underway to develop a pilot project.

Moreover, it is interesting to note that, in the 1990s, the NSA tested a comparable, privacy-protective surveillance system called "Operation ThinThread." ThinThread was said to be abandoned around the time of the 9/11 attacks. The reason for this, however, was not because it was ineffective. Reports indicated that other overriding, internal institutional priorities led to the loss of this positive-sum system, even though – we have been informed – it was highly effective at delivering on both privacy and security. (Incidentally, it was also said to be very cost-effective.)

Like Operation ThinThread, the multi-functional goal of *PPS* is to protect privacy, reduce false positives, and increase the efficiency of counter-terrorism surveillance. How would it work? A *PPS* system would scan relevant information environments (such as datasets, databases, or

networks) to detect instances of properly defined features or events associated with terrorist threats (as identified by intelligence experts) and analyze them, while remaining "blind" to the identities of all individuals (which would be encrypted) coexisting inside that environment. This privacy-preserving but powerful analytic approach would be achieved through the use of new encryption and Artificial Intelligence techniques which are able to efficiently analyze and encrypt data, as well as perform focused searches for terrorist-related activities.

As coordinated by the *PPS* system, intelligent virtual agents would amass encrypted profiles of potential terrorist threats by assembling and cross-referencing data associated with detected features. As profiles are assembled, they would be automatically analyzed for the probability of their being associated with an underlying terrorist threat. This would be done through the use of probabilistic graphical models (for example, a Bayesian network), which would weigh and map the connections between features of terrorist-related activities to isolate suspected threats. Since the graphical models would, in effect, be designed to amass evidence of suspected terrorist threats and do so in a manner that emulates the legal threshold required to obtain a warrant, the government would be in a position to take appropriate and timely steps to ensure the security of its citizens, while protecting the privacy of law-abiding citizens.

The only point at which the identity of any individual would be revealed would be after a *PPS*-empowered agency received a warrant from a court to decrypt the information. Obtaining this authorization would require that the agency satisfy the court that the agency had detected sufficient threat features to justify revealing the identity of the person or persons associated with the digital evidence. As indicated, this process would be greatly facilitated through *PPS*'s use of probabilistic graphical models. Throughout, neither the identities nor the personally identifiable information of law-abiding individuals would ever be revealed. In all cases, the collection of personally identifiable information would be minimized. To the extent that personally identifiable information would be collected, it would automatically be encrypted upon collection, and analyzed securely and effectively within the "space of cipher text," and then only divulged to the appropriate authorities with judicial authorization (a warrant). Moreover, at the end of a legally defined and limited period, all such information would be securely destroyed.

The necessary legal framework accompanying a *PPS* system would incorporate familiar mechanisms to allow a government to act quickly in exigent circumstances. So, for example, in a genuine emergency, a court would immediately make a time-limited auditable decryption key available to the agency, which in turn, would be required to return to the court to report on the circumstances justifying the exigent decryption.

While we are confident that a *PPS*-oriented approach is both relevant and necessary in the current context, we have no illusions that it must be backed up by providing critical institutions with the legal and technical resources necessary to ensure ongoing dynamic oversight. This point is driven home simply by reflecting on the recent revelations about intelligence agency efforts to weaken and break existing encryption standards. Strong encryption is absolutely essential,

but on its own, cannot be assumed to be sufficient. Indeed, technical safeguards must be accompanied by strong legal safeguards. These can and should be considered and implemented now, independently of the further work required to test and implement *PPS*. We turn to those vital legal elements next.

B. Transparency in Lawmaking

Transparency in lawmaking is essential to the health of any free and democratic society, particularly with respect to intrusive state powers. No country's citizens should be in doubt about the purpose or scope of their government's surveillance powers, let alone the functions, findings, and effectiveness of the courts and independent review bodies charged with overseeing the use of intrusive powers. Regrettably, legislators around the world have allowed their executive branches too much latitude, in a system designed to accommodate the secretive design and authorization of intrusive surveillance powers.

Intrusive surveillance tools without adequate safeguards have been referred to as "the spore of totalitarianism." While this no doubt sounds extreme, it is not without substance. Even if such disasters appear remote or hypothetical, history has taught us that injustice and tyranny are preceded by a rising tide of intrusion upon the privacy and dignity of ordinary citizens. During the 20th century, Americans fought off this tide both at home and abroad. Certainly the citizens of Germany have not forgotten what happened when secret police or intelligence agencies disregarded privacy. It is an integral part of their history and gives both young and old a critical perspective on state surveillance systems.

Meanwhile, even in free and open societies, sophisticated and readily available technologies add a whole new dimension to the state's power to subject its citizens to surveillance. In the words of former U.S. Supreme Court Justice William J. Brennan Jr., they make surveillance "more penetrating, more indiscriminate, more truly obnoxious to a free society. Electronic surveillance, in fact, makes the police omniscient, and police omniscience is one of the most effective tools of tyranny." The time to preserve our shared constitutional values is now, while we still enjoy a strong consensus about respect for human rights and the rule of law.

(i) The Role of Legislators

In our view, the Privacy and Civil Liberties Oversight Board should strongly encourage elected leaders to adopt a proactive approach to securing the rights affected by intrusive surveillance programs. In our view, it is not prudent to provide national security agencies with a 'blank check' that allows them to conceive of, design, and implement sweeping electronic surveillance programs, in near absolute secrecy. And yet this is exactly what appears to have been allowed to happen under provisions such as Section 215 of the *USA PATRIOT Act* and Section 702 of the *FISA Amendment Act*. Indeed, from what little we can tell thus far, the 'check' has been

'cashed' repeatedly vis-a-vis telephone and Internet metadata, financial data, and private email and social network contact lists, as well as the content of digital and Internet communications.

In the months ahead, if any such powers to conduct broad-based surveillance can be justified, they should be clearly defined under a statute. The governing statutory framework should include strong and explicit safeguards to help ensure that the purpose, nature, scope, and scale of the collection, use and retention of data is strictly controlled. As discussed above, access to the underlying personally identifiable information should also be supervised under a system of prior judicial authorization.

Nor should there be any mistake – these kinds of controls are as necessary with respect to communications metadata as they are with the content of our communications. As outlined in our July 2013 paper, *A Primer on Metadata: Separating Fact from Fiction* (attached), metadata surveillance programs facilitate the state's power to instantaneously create detailed digital profiles of the lives of anyone swept up in such massive data seizures. Once such data is compiled, detailed pictures of the lives of individuals begin to emerge that may easily be linked to places and events. The data can also reveal people's political or religious affiliations, as well as their personal and intimate relationships. Once such detailed individual pictures have been produced, if the individuals' identities are not already known, they can easily be determined with a few additional data sources.

Congress is already considering a number of bills designed to significantly restrict sweeping surveillance. Consideration should also be given to legislation that affirmatively sets out what forms of surveillance are permissible. In either case, the first priority for legislators should be to reassert their responsibility for publicly defining a clear legal framework.

(ii) The Role of the Judiciary

To date, the tasks assigned to the judiciary in the United States have placed FISC judges in the untenable role of approving large and novel surveillance *powers and programs*, in addition to authorizing focused *individual investigations*. As indicated above, legislators should be approving and circumscribing surveillance powers and programs, through explicit statutory enactments. The key role for the courts is to assess whether an agency can justify the use of intrusive power against precise statutory standards in a particular investigative context. It follows that the PCLOB should strongly encourage elected leaders to focus on realigning and sharpening the roles and responsibilities assigned to the FISC Court.

The PCLOB should also join others in calling for a much greater degree of transparency and accountability with respect to the FISC Court and its functions. To begin with, it is our view that all court decisions that determine legal issues related to the authority, scope and necessary safeguards for surveillance programs, operations, and investigations, should be made public. We also strongly support calls for the creation of a new privacy and civil liberties advocate to

challenge the government's case for spying. Further, all multi-dimensional legal questions should be resolved by three judges, randomly assigned to three-member panels. If a panel splits two-to-one, the dissenter and the privacy/civil liberties advocate should both have the right to ask the court to decide the case "en banc" (by the full panel of the court). In addition, the privacy/civil liberties advocate should have the statutory authority to appeal an "en banc" decision to the U.S. Supreme Court.

C. Additional Mechanisms to Ensure Accountability

It should now be evident that we cannot take much comfort from the fact that intelligence agencies currently face a degree of scrutiny from the judicial, legislative, and executive branches of government, particularly where that supervision has been structured so as to leave security agencies with far too much control over what information these coordinate branches of government have access to and whether any of that information will ever be made public. Most intelligence operations are necessarily conducted in secret. However, the need for operational secrecy must not stand in the way of public accountability. The absence of sufficient measures to ensure accountability poses a serious threat to privacy and the preservation of our freedoms.

In our view, what is needed is a legal requirement that agency surveillance programs are built with internal access and audit controls designed to verify compliance with the law, that are hard wired into agency systems. In addition, the judicial, executive, and congressional bodies tasked with overseeing national security surveillance programs must have automatic access to the resulting regular (monthly) audit reports, as well as the necessary resources to allow them to raise and obtain answers to their questions about the information they receive. This means that they must have access to sufficient numbers of dedicated, security-cleared, expert audit staff. Led by a Chief Security Auditor (CSA), such staff must have explicit authority to access every agency's audit tools, but be independent of the security agencies themselves.

Accordingly, the CSA should be appointed by the President, on the approval of the Senate. The term should be sufficiently long to ensure that members of the FISC Court and Congress receive expertise, reporting, and advice from an office with the continuity and experience required in this complex area. Ultimately, the CSA should report to, answer to, and be funded by Congress, and only be dismissible for cause.

Finally, members of both the FISC Court and Congress must, at a minimum, be legally entitled to publicly state the general nature of their concerns about the legality and propriety of current and proposed surveillance programs and practices. This is critical to ensuring that intelligence agencies remain accountable to the public they serve.

4. Conclusion

We readily acknowledge the need for effective measures to counteract terrorism and other threats to national security. However, the ongoing revelations concerning the state's indiscriminate collection of vast amounts of data on domestic and international communications oblige us, as members of free and open societies, to ask essential questions – not only to question the legitimacy of these counter-terrorism measures, but to attempt to redesign them in a way that respects the privacy of all law-abiding individuals.

Fortunately, we believe that it is possible to develop an approach that is fully capable of protecting both security and privacy. It is to this end that this submission is offered today. We believe a unique opportunity exists to carve out a new approach. If we build a system of dynamic symmetrical oversight, based on transparency in lawmaking, effective mechanisms to ensure accountability, and *Privacy-Protective Surveillance*, we believe Americans will be able to protect national security at "home," while inspiring nations around the world to secure citizens' privacy and freedom everywhere. The time to lead the way is now.

Should you have any questions regarding our submission or require assistance with any of the content, we are fully prepared to offer our help in any way.

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner,
Ontario, Canada

October 22, 2013

Date