www.jusletter-it.eu

Ann Cavoukian

# Canada's Secretive Work with the NSA Demonstrates the Need for Privacy-Protective Surveillance

The revelations from the Edward Snowden have made it very clear that significant change is needed in the ways that the intelligence agencies such as the Communications Security Establishment Canada (CSEC) and National Security Agency (NSA), operate and are overseen. The article proposes a new methodology called Privacy-Protective Surveillance (PPS) which offers a positive-sum, «win-win» alternative to the current invasive, counter-terrorism surveillance systems.

Category: Articles
Field of law: Data Protection; Data Security
Region: Kanada

Citation: Ann Cavoukian, Canada's Secretive Work with the NSA Demonstrates the Need for Privacy-Protective Surveillance, in: Jusletter IT 15 May 2014

[Rz 1] Until the revelations of the Edward Snowden documents, Canadians had been almost completely in the dark about the activities of their spying agencies, in particular, Canada's cryptologic counterpart to America's National Security Agency (NSA), the Communications Security Establishment Canada (CSEC). Both agencies are members of the «Five Eyes», a signals intelligence (often shortened to SIGINT) alliance. Communication intelligence agencies from Australia, New Zealand, and the United Kingdom make up the rest of the group. This alliance shares information and secretly works to both protect the information technology systems of their countries and intercept foreign communications which may present threats to domestic security.

[Rz 2] Though specific details of CSEC's work with the «Five Eyes» have been few and far between, what has emerged from the Snowden documents has been surprising and has begun to shed light on how extensive these collaborations are. One of the most disconcerting revelations so far is the key role Canada played in weakening the encryption standards of the Internet, thus weakening the privacy and security of all of our digital communications. This type of action is exactly why citizens of free and democratic societies need to demand transparency and accountability, as well as respect to privacy protections such agencies and their surveillance programs and activities. First, however, the challenge is to understand what these agencies are capable of and the methods they have used to obtain information.

[Rz 3] From what we can tell, Canada's intelligence work on weakening the encryption standards of the internet transpired back in the mid-2000s on a project known as «Bullrun.» Media reports indicate that CSEC was heading up the standards development process for the Cryptographic Module Validation Program (CMVP). This program is an ongoing joint venture between the U.S. National Institute of Standards and Technology (NIST) – which the NSA participates in – and CSEC. The CMVP produced a list of approved algorithms for encryption that were «accepted for the protection of sensitive information» by NIST, which were later adopted by the International Organization for Standardization (which counts 163 countries as members). For more than six years, one of the principal algorithms listed was the Dual Elliptic Curve Deterministic Random Bit Generator (Dual_EC_DRBG), which generated the random numbers that form the foundations of such an encryption program.

[Rz 4] Dual_EC_DRBG was different from other programs as it had a built-in backdoor which rendered the encryption vulnerable to hacking. The patent application filed for the algorithm's underlying technology by Canada's Certicom Corporation in 2005 described it as including a set of [secret] keys that could be used, for example, by «trusted law enforcement agents» to defeat the encryption. The original patent application drew little attention; however, in 2007, when Dual_EC was added to the NIST list, it started to draw some concern. Two Microsoft researchers rediscovered that when implemented in the real world, it still contained a version of the backdoor as described in the patent. No one knew if anyone had the secret key, but the very existence of such a backdoor caused security researchers to try and boycott Dual_EC. One of the world's leading cryptographers, Bruce Schneier said, «while we were saying don't use it, government contractors were demanding it». Snowden finally revealed last year that the NSA was the holder of the Dual_EC secret keys which allowed the spy agency to crack that encryption scheme at will. Researchers now question what other backdoors have yet to be discovered.

[Rz 5] And this may just be the tip of the iceberg for Canada's involvement in global as well as domestic surveillance. Subsequent Snowden documents have revealed CSEC and the NSA collaborated to spy on foreign heads of state in Toronto at the G8 summit. Even more troubling, CSEC conducted a WiFi-facilitated, warrantless surveillance operation in 2012. The operation involved

the processing of at least two weeks of identifying information associated with mobile devices. The operation involved locating users backward and forward in time within a major Canadian international airport and other airports, as well as, hotels and mobile gateways in many cities. It was reported that the operation was simply a trial run of a powerful new «needle in a hay stack» analytic software program designed to obtain richer contextual data which CSEC developed with help from the NSA. A CSEC document recently released by Edward Snowden indicates that this trial run was part of «a 5-Eyes effort to enable the SIGINT system to provide real-time alerts of events of interest». Many key questions remain. Was this program legal? How much of this Canadian-focused metadata does CSEC collect and why? How long does it retain this data and for what purposes? Has the program been used again? Who are they disclosing metadata to and why?

[Rz 6] No country's citizens should be in doubt about the scope of their government's surveillance agencies mandate and powers. Regrettably, legislators around the world have allowed these agencies too much latitude to develop intrusive surveillance programs in near absolute secrecy.

[Rz 7] Indeed, our government, like many others, has been tight-lipped about these issues. Very little clarity has been provided about the nature and scope of CSEC's surveillance programs. It is time that free societies receive clear answers to these kinds of questions. Political leaders must not be coy about the size, scope, or purpose of their intelligence programs lest they run the risk of undermining citizens» trust in government. This manifests itself in the growing distrust of government that exists today. I feel, as do many others, that the state's «trust us» model is wearing thin. It remains my view that we can and must have a legal framework that allows for necessary surveillance, provides clear and strong privacy protections, and delivers on accountability and transparency. In the meantime, warrantless mass surveillance must end.

[Rz 8] As we are calling for an end to systems of warrantless mass surveillance, we must, in turn, explore new ideas and rethink our approach to providing necessary security. Above all, privacy, the ability of law-abiding citizens to control the collection, use, and disclosure of their personal information – referred to at times as «informational self-determination» – must be protected in any SIGINT system.

[Rz 9] As one solution to this complex problem, I worked with Professor Khaled El Emam on a new concept for surveillance that we call Privacy-Protective Surveillance (PPS)[1]. This new methodology offers a positive-sum, «win-win» alternative to current counter-terrorism surveillance systems. Most measures to counteract terrorism seek to strike a «balance» between public safety and privacy. This often leads to engaging in a zero-sum paradigm of giving up what is perceived to be the «less important value», privacy, in favor of the «more significant value», public safety. This zero-sum trade-off is invariably destructive in free and open societies. It is not only inappropriate, it is unnecessary.

[Rz 10] Privacy-Protective Surveillance builds on *Privacy by Design*, the international framework recognized as «an essential component of fundamental privacy protection» by Data Protection and Privacy Commissioners in 2010. By embedding privacy directly into its design and architecture, through the use of such technologies as intelligent virtual agents, homomorphic encryption, and machine-learning data analysis networks, PPS allows for privacy and counter-terrorism mea-

[1] Introducing Privacy-Protective Surveillance: Achieving Privacy and Effective Counter-Terrorism (available at: http://www.realprivacy.ca/index.php/paper/introducing-privacy-protective-surveillance-achieving-privacy-effective-counter-terrorism/).

sures to co-exist in tandem, without diminishing the intelligence-gathering capabilities of the systems involved.

[Rz 11] The multi-functional goal of PPS is to protect privacy by only allowing access to data under encryption and reducing false positives. A PPS system scans relevant information environments (such as datasets, databases, or networks) to detect instances of pre-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 strongly encrypted) coexisting inside that environment. 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 a sufficient and credible threat. A PPS approach also includes additional independent checks and balances that verify whether security measures are being implemented alongside necessary privacy protections. Such a model could be adopted so as to protect individual privacy of residents and «overseas» persons alike.

[Rz 12] Privacy and counter-terrorism measures can co-exist, with both values being respected. We know this is possible to achieve! Indeed, we possess the technology and can develop the system design to achieve this positive-sum or doubly-enabling end result. By doing so, we will be able to implement strong counter-terrorism measures, while ensuring the future of freedom and liberty. We must engage citizens across the world so that the message of «respect our privacy, respect our freedoms», can be heard, loud and clear. In free and open societies, we deserve no less.

---

Dr. Ann Cavoukian is the Information & Privacy Commissioner of Ontario, Canada. Her full paper on Privacy-Protected Surveillance can be downloaded from realprivacy.ca (please note, the paper is currently only available in English).