Surveillance Technologies: Privacy in Public Spaces

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner
Ontario, Canada

IEEE
International Symposium on Technology and Society
Toronto, Canada
June 28, 2013
Privacy = Freedom
Entering into an Era of Expanded Surveillance

• NSA/PRISM/Big Data-Metadata
• Drones/Unmanned Ariel Vehicles (UAVs)
• Automatic Licence Plate Scanners (ALPs)
• Vehicle Black boxes/GPS
• Video Surveillance (CCTV)
• Biometric Tracking
• Legislation (Bill C-30)
Landmark Resolution Passed to Preserve the Future of Privacy


JERUSALEM, October 29, 2010 – A landmark Resolution by Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, was approved by international Data Protection and Privacy Commissioners in Jerusalem today at their annual conference. The resolution recognizes Commissioner Cavoukian's concept of Privacy by Design - which ensures that privacy is embedded into new technologies and business practices, right from the outset - as an essential component of fundamental privacy protection.

Full Article:
http://www.science20.com/newswire/landmark_resolution_passed_preserve_future_privacy
Privacy by Design: Proactive in 31 Languages!

1. English
2. French
3. German
4. Spanish
5. Italian
6. Czech
7. Dutch
8. Estonian
9. Hebrew
10. Hindi
11. Chinese
12. Japanese
13. Arabic
14. Armenian
15. Ukrainian
16. Korean
17. Russian
18. Romanian
19. Portuguese
20. Maltese
21. Greek
22. Macedonian
23. Bulgarian
24. Croatian
25. Polish
26. Turkish
27. Malaysian
28. Indonesian
29. Danish
30. Hungarian
31. Norwegian
Positive-Sum Model

Change the paradigm from a zero-sum to a “positive-sum” model:
Create a win-win scenario, not an either/or (vs.) involving unnecessary trade-offs and false dichotomies …

replace the “vs.” with “and”
Privacy by Design: The 7 Foundational Principles

1. **Proactive not Reactive:**
   Preventative, not Remedial;

2. Privacy as the **Default** setting;

3. Privacy **Embedded** into Design;

4. **Full** Functionality:
   Positive-Sum, not Zero-Sum;

5. **End-to-End Security:**
   Full Lifecycle Protection;

6. **Visibility and Transparency:**
   Keep it Open;

7. **Respect for User Privacy:**
   Keep it User-Centric.

Privacy by Design is a concept developed back in the 90’s, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks: rather, privacy assurance must ideally become an organization’s default mode of operation.

Initially deploying Privacy-Enhancing Technologies (PET) was seen as the solution. Today, we realize that a more substantial approach is required — encoding the use of PETs to PETs Plus — taking a positive-sum (full functionality) approach, not zero-sum. That’s the “Plus” in PETS Plus: positive-sum, not the either/or of zero-sum (a false dichotomy).

Privacy by Design extends to a “Trilogy” of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure.

Principles of Privacy by Design may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy measures tends to be commensurate with the sensitivity of the data.

The objectives of Privacy by Design — ensuring privacy and gaining personal control over one’s information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following 7 Foundational Principles (see over page):
Operationalizing Privacy by Design

9 PbD Application Areas

• CCTV/Surveillance cameras in mass transit systems;
• Biometrics used in casinos and gaming facilities;
• Smart Meters and the Smart Grid;
• Mobile Communications;
• Near Field Communications;
• RFIDs and sensor technologies;
• Redesigning IP Geolocation;
• Remote Home Health Care;
• Big Data and Data Analytics.

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner,
Ontario, Canada

December 2012
OASIS Technical Committee – *Privacy by Design for Software Engineers*

- Commissioner Cavoukian and Professor Jutla are serving as Co-Chairs of a new technical committee (TC) of OASIS (Advancing Open Standards for the Information Society) – *PbD-SE* (software engineers) TC;
- The purpose of *PbD-SE* is to provide *PbD* governance and documentation for software engineers;
- The *PbD* standards developed will pave the way for software engineers to code for *Privacy, by Design*. 
Carnegie Mellon University – Privacy By Design

- New Master's degree program for privacy engineers to be offered by Carnegie Mellon University, School of Computer Science;
- The Master of Science in Information Technology-Privacy (MSIT-Privacy) is a 12-month program that begins in the fall semester of 2013;
- The program will emphasize the concept of Privacy by Design, in which safeguards are incorporated into the design of systems and products from the very beginning of the development process;
- Students who complete the master's program will be prepared for the International Association of Privacy Professionals (IAPP) Certified Information Privacy Professional certification exam.
Surveillance
Beware of *Surveillance by Design*

- **Summer, 2011** – One of the greatest threats to privacy actually materialized from within my own federal government – *Bill C-30* – which would have enabled *warrantless access* by law enforcement;

- Throughout our opposition to *Bill C-30*, I referred to the proposed warrantless access as a system of “*Surveillance by Design.*”
Give Me Real Privacy
NOT
PRIVACY THEATRE

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner
Ontario, Canada

www.RealPrivacy.ca
Commissioner’s Op-Ed: [Un]Lawful Access

Privacy Commissioner Ann Cavoukian: Privacy invasion shouldn’t be ‘lawful’

We should not allow government to violate our right to be secure from unreasonable state surveillance

By Ann Cavoukian

I must add my voice to the growing dismay regarding the impact of impending “lawful access” legislation in this country. In my view, it is highly misleading to call it “lawful.” Let’s call it what it is — a system of expanded surveillance.

At issue is the anticipated re-introduction of a trio of federal bills that will provide police with much greater ability to access and track information, via the communications technologies we use every day, such as the Internet, smart phones and other mobile devices. I have no doubt that, collectively, the legislation will substantially diminish the privacy rights of Ontarians and Canadians as a whole.

Let’s take a brief look at the surveillance bills, which were introduced prior to the last election:

- Bill C-40 would make it easier for the police to obtain judicial approval of multiple intercept and tracking warrants and production orders, to access and track e-communications.
- Bill C-41 would give the police new powers to obtain court orders for remote live tracking, as well as suspicion-based orders requiring telecommunication service providers and other companies to preserve and turn over data of interest to the police.
- Bill C-42 would require telecommunication service providers to build and maintain intercept capability into their networks for use by law enforcement, and give the police warrantless power to access subscriber information.

I well understand the attraction for law enforcement officials — the increased ability to access and track e-communications, with reduced judicial scrutiny, would put a treasure trove of new information at their fingertips.

However, we must be extremely careful not to allow the admitted investigative needs of police forces to interfere with or violate our constitutional right to be secure from unreasonable state surveillance. The proposed surveillance powers come at the expense of the necessary privacy safeguards guaranteed under the Charter of Rights and Freedoms. The federal government must be persuaded to acknowledge the sensitivity of traffic data, stored data and tracking data, and strongly urged to re-draft the bills. For a start, the proposal for warrantless access to subscriber information is untenable and should be withdrawn. If such access to subscriber information is considered to be absolutely necessary, it must take place under a court-supervised regime.

The government needs to step back and consider all of these implications. A comprehensive cost-benefit analysis should precede the advancement of so many significant public policy decisions. Public Parliamentary hearings must also be scheduled to ensure that civil society, as well as the telecom industry, has a full opportunity to provide input.

Canadians must press the federal government to publicly commit to enacting much-needed oversight legislation in tandem with any expansive surveillance measures. Intrusive proposals require, at the very least, matching legislative safeguards. The courts, affected individuals, future Parliamentarians and the public must be well informed about the scope, effectiveness and damaging negative effects of such intrusive powers.

We can, and must, have both greater security and privacy. It cannot be one at the expense of the other. The true value of privacy must be recognized in any effort to modernize law enforcement powers. Imposing a mandatory surveillance regime on the public and its telecom service providers must not go forward without strong safeguards to protect the fruits of our fundamental freedoms.

National Post

Ann Cavoukian is the Information Privacy Commissioner of Ontario.
Demise of Bill C-30

Harper government kills controversial Internet surveillance bill

JOHN IBBITSON
Ottawa — The Globe and Mail
Published Monday, Feb. 11 2013, 3:42 PM EST
Last updated Tuesday, Feb. 12 2013, 9:57 AM EST

The Harper government will not resurrect its controversial Internet surveillance bill, and will not introduce new legislation to monitor the activities of people on the web.

The bill, which excited outrage over possible privacy violations on the Internet, marks a legislative failure for the Harper majority government.

MORE RELATED TO THIS STORY

• JOHN IBBITSON Can Conservatives resurrect the Internet surveillance bill?
• SURVEILLANCE Can Internet snooping protect us, or do criminals just get used to it?
• Telcos in talks with Ottawa to shape Internet 'spy' bill: documents

“We’ve listened to the concerns of Canadians,” Justice Minister Rob Nicholson told reporters outside the House of Commons on Monday.

He said that “we will not be proceeding with Bill C-30. And any attempts to modernize the criminal code will not contain warrantless...
What About Terrorism?
“Boston Bombings Spur Calls for More Surveillance Measures”

• In the wake of the Boston Marathon bombings, calls for increased camera surveillance in the U.S. have increased;

• Lawmakers think the use of a better-connected system of cameras, controlled by law enforcement, may have helped speed up the suspects' identification.

— Wall Street Journal, Call for More Video Cameras Spotlights Debate on Use, April 19, 2013.

http://online.wsj.com/article/SB10001424127887324763404578433143080413704.html#printMode?KEYWORDS=spur+calls
“Support for public surveillance cameras may be up substantially over the past decade, but Americans are warier than ever about government monitoring of their private cell-phone and e-mail communications, with 59% opposed to such actions.”


http://swampland.time.com/2013/05/01/homeland-insecurity-after-boston-the-struggle-between-liberty-and-security/
Would you be willing to give up some civil liberties if that were necessary to curb terrorism?

Zeke J. Miller,
*Poll: Americans More Concerned About Civil Liberties In Wake Of Boston Bombing,*
Time Magazine, May 1, 2013.
http://swampland.time.com/2013/05/01/poll-americans-more-concerned-about-civil-liberties-in-wake-of-boston-bombing/#ixzz2SF3efpro
Do you favor increased powers of investigation that law-enforcement agencies might use when dealing with suspected terrorists?

Zeke J. Miller,
Poll: Americans More Concerned About Civil Liberties In Wake Of Boston Bombing,
Time Magazine, May 1, 2013.
http://swampland.time.com/2013/05/01/poll-americans-more-concerned-about-civil-liberties-in-wake-of-boston-bombing/#ixzz2SF3efpro
Surveillance Technologies and Privacy
SURVEILLANCE, THEN AND NOW: Securing Privacy in Public Spaces

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner
Ontario, Canada
June 2013

www.privacybydesign.ca
A ‘Wait And See’ Approach is No Longer Sufficient ...

- Emerging issues that raise substantial privacy concerns, in addition to CCTV surveillance cameras, include GPS tracking, automatic license plate recognition systems, and more recently, drone-based surveillance;
- The end of “practical obscurity” cannot in any way signal an end to our right to privacy;
- Privacy is being transformed with the rise of PbD to proactively strengthen the protection of our personal data, and our freedoms.
It is One Thing to Be “Seen” in Public – It is Another to Be Tracked by the State

• Public spaces facilitate a range of vital activities in a democratic society: transportation, recreation, shopping, socializing, and artistic performance;

• **Warrantless** surveillance that facilitates the sustained tracking of people engaging in everyday activities in public spaces is unacceptable in freedom loving countries;

• In Canada’s Supreme Court, Justice La Forest referred to such warrantless surveillance as being “unthinkable:” “It is an unthinkable prospect in a free and open society such as ours.”
Privacy by Design is an excellent idea. Designing administrative means to protect personal privacy before it is breached is a welcome addition to the tools for protecting this vitally important human value."

— The Honourable Justice Gérard Vincent La Forest, QC, Justice of the Supreme Court of Canada, 1985-1997
Drones and Domestic Surveillance

- On Feb. 14th, President Obama signed the *FAA Modernization and Reform Act* into law. The Act is largely focused on ensuring funding for the FAA, but also allows the FAA to permit the domestic use of drones and requires testing and licensing regulations by 2015;
- The FAA estimates that as many as 30,000 drones could be in use by 2020;
- On February 13th, the *Preserving American Privacy Act, 2013* (PAPA) was introduced by three Congressional Representatives and is now before the House Subcommittee on Crime, Terrorism, Homeland Security and Investigations;
- **PAPA** focuses on requiring prior judicial authorization for law enforcement uses of drone-based surveillance except in very limited circumstances.
Drones and Domestic Surveillance (Cont’d)

- 28 U.S. states are actively consulting bills intended to restrict the use of drones for purposes of domestic surveillance, the majority of which will require a warrant;
- The Virginia legislature has passed a two-year moratorium on drone use;
- 5 states – Florida, Idaho, Montana, Tennessee and Texas, have already enacted warrant requirements.

NSA/CSEC and Surveillance

www.privacybydesign.ca
NSA/CSEC

- **June, 2013** – It was revealed that the National Security Agency (NSA) is collecting the telephone records of tens of millions of American customers of various telecoms under top-secret FISA court orders;

- It was later discovered that technology companies such as Google, Microsoft and Apple were involved with U.S. national security officials in the collection of emails, videos and other documents over the last six years – amassing a database of personal information;

- Privacy Commissioner of Canada, Jennifer Stoddart, indicated that she will be looking into the implications for Canadians, including the involvement of Communications Security Establishment Canada (CSEC) – the Canadian counterpart to the NSA.
The 'Me' in Metadata

Almost every digital file we generate carries invisible tags.

**Metadata Examples**
- Focal length
- Camera type taken
- Date & time taken
- Exposure
- Flash setting
- Internet provider
- Mail client
- IP address
- Preferred language
- Location
- Place ID

**From the tweet:**
- Coordinates: 42.59640 -114.4012
- Language: EN

**From the email:**
- Date/Time: 2013: 04: 22 15: 57: 33

**From the photo:**
- Camera Type: HTC One X
- Flash Setting: AUTO

**1.** Geoff poses by a waterfall and snaps a self-portrait, which he immediately tweets, then emails to his grandmother.

**2.** Geoff’s text, photo, and email ascend to a series of remote servers, each dragging their own trails of metadata.

**3.** Once there, the metadata may be extracted and interpreted by any interested party with access.

Thanks to the above metadata, without ever having met Geoff, we know he was at Shoshone Falls near Twin Falls, Idaho, at 3:57 p.m. on April 22, that he has an HTC One X smartphone, and that he is an English language speaker.

Note: Actual metadata code modified for readability. Many metadata values, such as time, can be extracted from multiple sources, and values may differ slightly.

Source: staff reporting

The Wall Street Journal
Judicial Authorization

• Law enforcement’s power to gather information from third parties to identify individuals engaged in activities of interest to the state must be subject to timely, independent scrutiny in the form of the appropriate combination of prior judicial authorization and/or subsequent notice, reporting, and accountability requirements;

• We can and must have both effective law enforcement and rigorous privacy protections. Eternal vigilance will be required to secure our fundamental rights, including the right to privacy in relation to all public spaces, including those found online and in virtual spaces.

— Commissioner Ann Cavoukian, Surveillance, Then and Now: Securing Privacy in Public Places, June, 2013
Senior government officials are defending the systemic seizure of personal information on the basis that “metadata” is neither sensitive nor private. Given the implications for privacy and freedom, it is critical that we question the dated, but dangerously prevalent, zero-sum approaches to privacy and security. We must reject the view that in order to have security, we must give up our right to privacy. We do not.
Privacy-Protective Surveillance
Privacy Meets Artificial Intelligence
Objectives for privacy-protective surveillance

• The ability to scan the Web and related databases to find digital evidence relating to potentially suspicious criminal activity by some, without infringing on the privacy of other unrelated individuals.

• A technological infrastructure to ensure that any personally identifying information on any unsuspected individuals is not collected and, in those associated with targeted activity, PII is only divulged with judicial authorization (a warrant).
Multi-agents tailored to search for specific features

Multi-agent search engine
What is a feature?

A specific type of information or data correlation which, when combined with other features, may indicate suspicious behaviour that would warrant further investigation.
What is being stored if a feature is detected for an individual?

1. That a feature was detected;
   (A feature detector is, in effect, “blind” to anything other than the feature it was designed to detect);

2. Encrypted personal data: one’s identity, the time and place of occurrence (if relevant), and the context.
Concluding Thoughts

• Beware of the steady creep of surveillance technologies, expanding into a growing number of devices;

• Ensure that surveillance is accompanied by privacy measures, embedded by design, into IT systems and operational processes;

• Surveillance measures by the state must be accompanied by judicial authorization;

• Get smart – lead with Privacy – by Design, not privacy by chance or, worse, Privacy by Disaster!
How to Contact Us

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario, Canada
M4W 1A8
Phone: (416) 326-3948 / 1-800-387-0073
Web: www.ipc.on.ca
E-mail: info@ipc.on.ca

For more information on Privacy by Design, please visit: www.privacybydesign.ca