

Privacy By Design: Paving the Way to Privacy-Protective Surveillance

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario, Canada

Queen's University

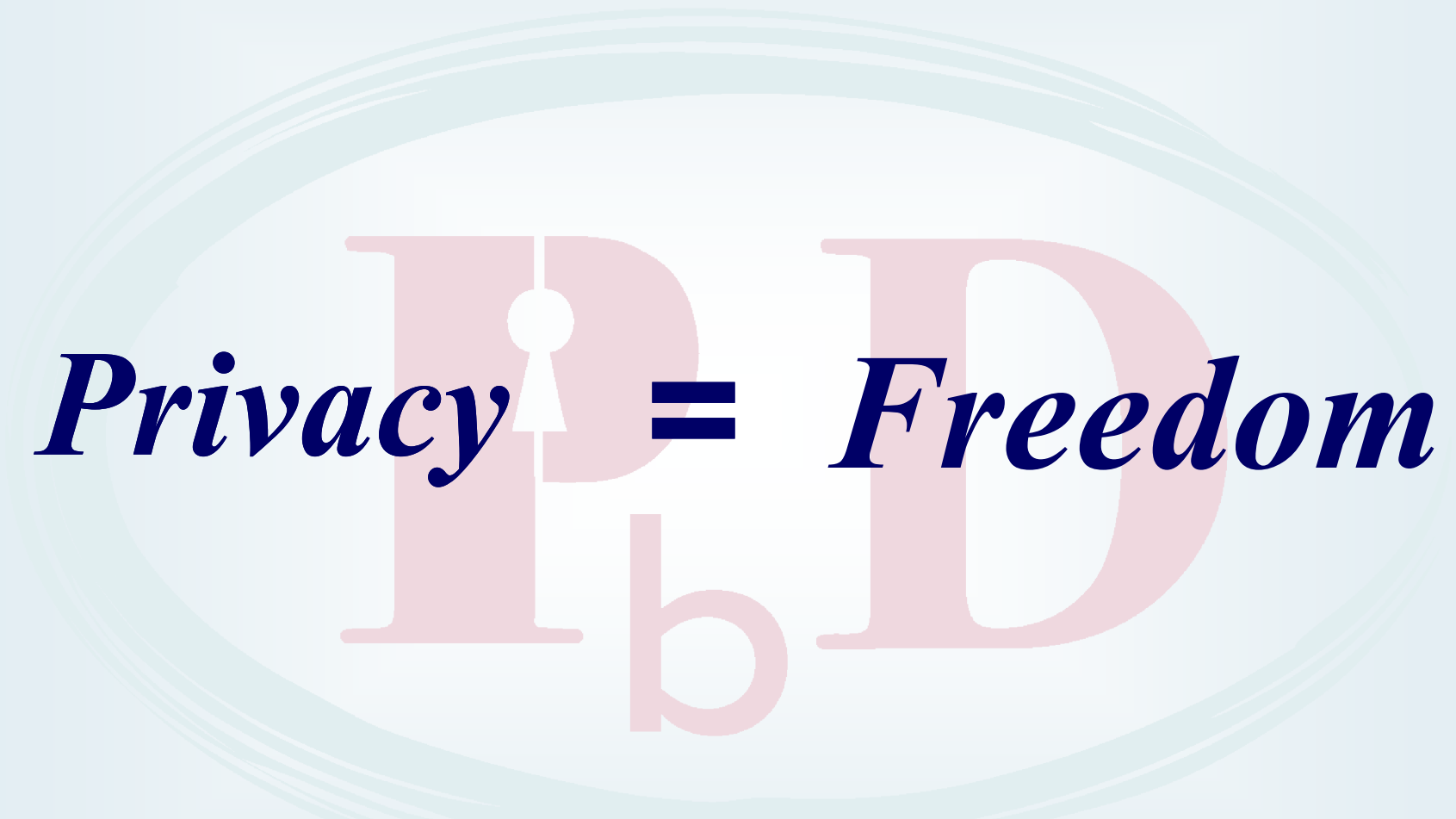
Kingston, Ontario

September 10, 2013

www.privacybydesign.ca

Presentation Outline

- 1. Entering an Era of Expanded Surveillance*
- 2. Privacy by Design: The Gold Standard*
- 3. Beware of Surveillance by Design*
- 4. What About Counter-Terrorism?*
- 5. Surveillance Technologies and Privacy*
- 6. Privacy-Protective Surveillance, by Design*
- 7. Concluding Thoughts*



Privacy **=** *Freedom*

The text is centered within the oval. The word "Privacy" is in a dark blue, italicized serif font. The word "Freedom" is also in a dark blue, italicized serif font. Between them is a bold, black equals sign. The letters "P" and "D" are rendered in a large, light red, serif font, with the "P" partially overlapping the "D". A small white keyhole icon is positioned on the vertical stem of the "P". Below the "P" and "D" is a smaller, light red lowercase letter "b".

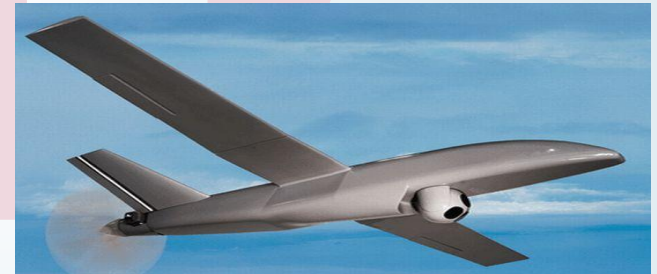
www.privacybydesign.ca

Privacy = Control

www.privacybydesign.ca

Entering into an Era of Expanded Surveillance

- NSA/PRISM/Metadata
- Drones/Unmanned Ariel Vehicles (UAVs)
- Automatic Licence Plate Scanners (ALPs)
- Vehicle Black boxes/GPS
- Video Surveillance (CCTV)
- Biometric Tracking
- Legislation (Bill C-30)



The Decade of Privacy by Design



www.privacybydesign.ca

Adoption of “Privacy by Design” as an International Standard

Landmark Resolution Passed to Preserve the Future of Privacy

By Anna Ohlden – October 29th 2010 - http://www.science20.com/newswire/landmark_resolution_passed_preserve_future_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

The 7 Foundational Principles

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

Privacy by Design is a concept I 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 (PETs) was seen as the solution. Today, we realize that a more substantial approach is required — extending 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.

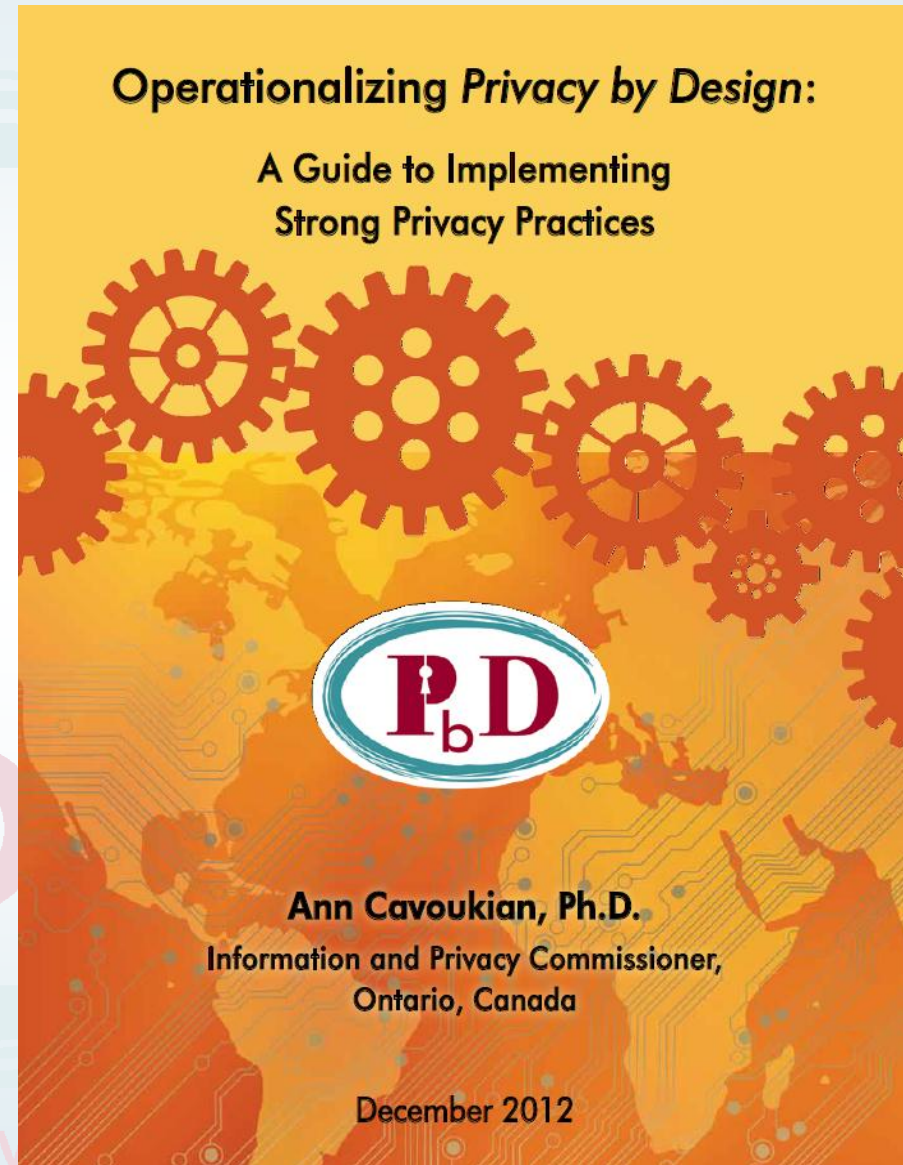
Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy measures tends to be commensurate with the sensitivity of the data.

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.



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.



***Beware of
Surveillance by Design***

www.privacybydesign.ca

Beware of *Surveillance by Design*

- **Summer, 2011** – One of the greatest threats to privacy actually materialized from within our own government – *Bill C-30* – which would have enabled *warrantless access* by law enforcement;
- My office launched a campaign opposing *Bill C-30*, in which I referred to the proposed warrantless access as a system of “*Surveillance by Design.*”

Give Me RealPrivacy

NOT

PRIVACY THEATRE

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

www.RealPrivacy.ca

Commissioner's Op-Ed: [Un]Lawful Access


nationalpost.com | financialpost.com | Today's Paper | Delivery | Contact | Digital Paper | Sign In | Register Today

NATIONAL POST

National Post | Full Comment | Canada | Environment | Letters | Policy | Pop Culture | Social Issues | U.S. Politics | World Politics

FULLCOMMENT

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. foto

National Post Oct 31, 2011 — 7:30 AM ET | Last Updated: Oct 27, 2011 4:32 PM ET

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-50 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-51 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-52 would require telecommunication service providers to build and maintain intercept capability into their networks for use by law enforcement, and gives the police warrantless power to access subscriber information.

I well understand the attraction for law enforcement officials — the increased ability to access and track our 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 special 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 entrenchment 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 Parliaments 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, in unison. 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 future of our fundamental freedoms.

National Post

Ann Cavoukian is the Information Privacy Commissioner of Ontario.



Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, ON M4W 1A8
CANADA

Tel: 416-326-3333
Toll-free: 1-800-387-0073
Fax: 416-326-9195
Email: info@ipc.on.ca
Website: www.ipc.on.ca

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

347 comments

695 457 224 14 +1 29 Print / License AA



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



VIDEO
Video: Government

"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
Counter-Terrorism?***

www.privacybydesign.ca

Boston Marathon Bombings

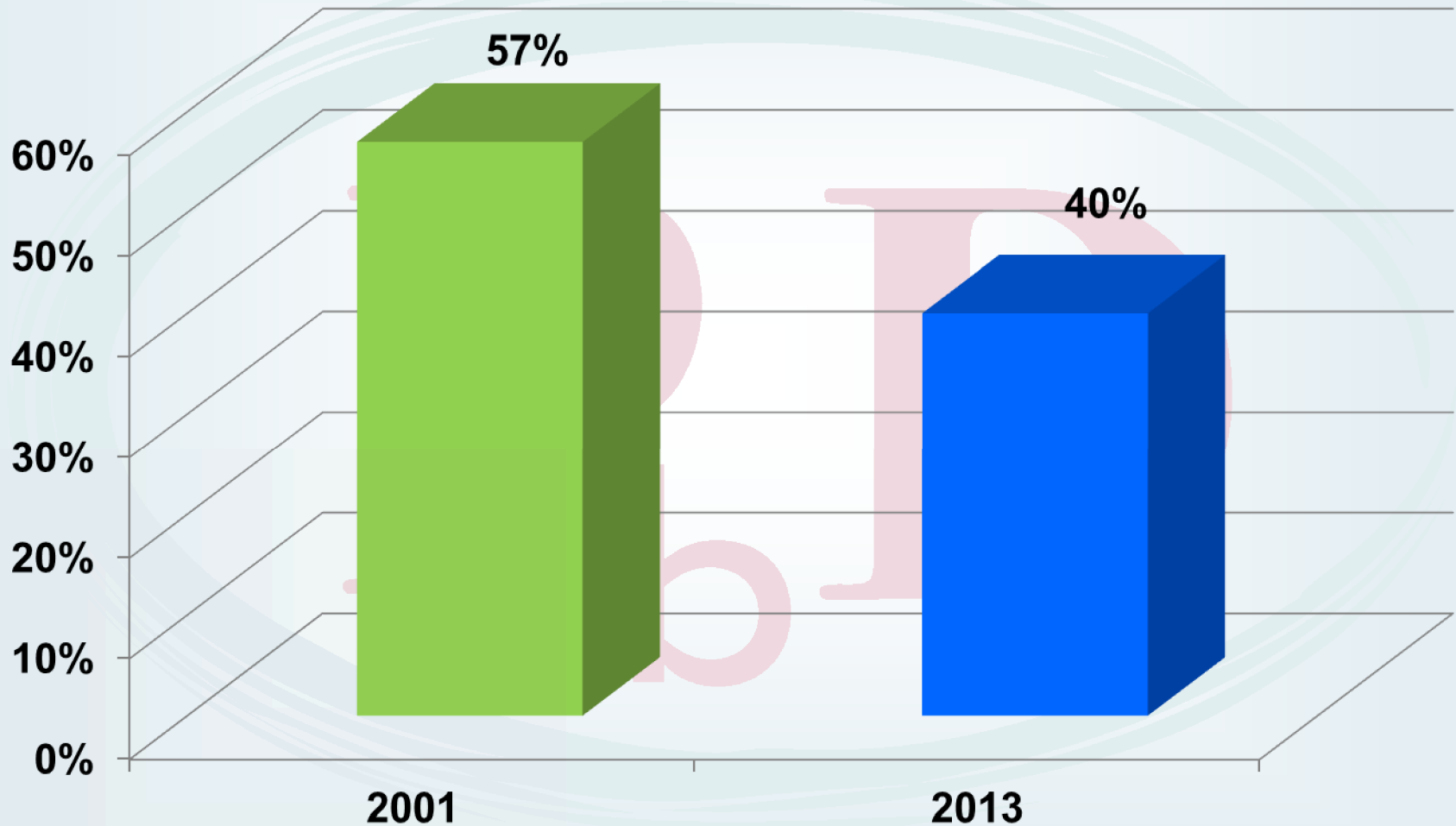
“Support for surveillance cameras may be up substantially over the past decade, but Americans are warier than ever about government monitoring of their private cell-phone and e-mail communications, with 59% opposed to such actions.”

— Massimo Calabresi and Michael Crowley,
Homeland Insecurity: After Boston, The Struggle Between Liberty and Security,
Time Magazine, May 1, 2013.



<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?

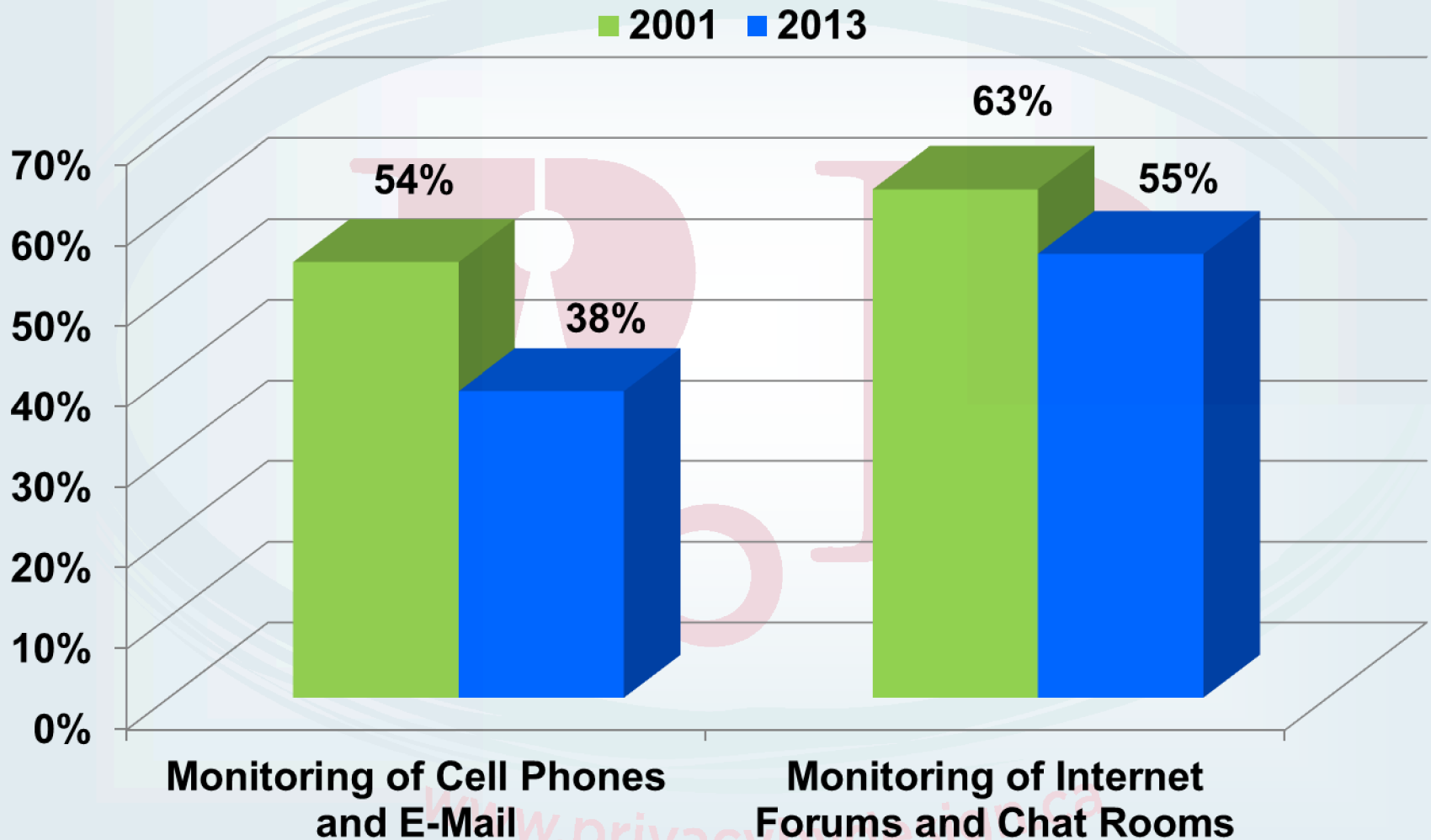


www.privacybydesign.ca

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>

A large, light blue, stylized eye graphic with multiple concentric lines forming the iris and eyelids, centered in the background. The text is overlaid on this graphic.

***Surveillance Technologies
and Privacy***

www.privacybydesign.ca



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 in Law, Policy and Practice

“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

A large, light blue, stylized eye graphic with multiple concentric lines forming the iris and pupil, centered on the page. The text is overlaid on this graphic.

NSA/CSEC
and Surveillance

www.privacybydesign.ca

CSEC/NSA

- **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;
- Canadians are urgently demanding answers from the government after a report by independent CSE watchdog and retired judge Robert Decary revealed the potentially illegal spying during a review of CSEC's activities over the past year.

CSEC/NSA

- The CSEC is forbidden by law to spy on Canadians, no matter where they are in the world;
- OpenMedia.ca is calling on Canadian telecom companies to make clear whether they are involved in facilitating agencies like CSEC to spy on the private Internet activities of Canadian residents;
- The NSA is said to be intercepting online communications, e-mails, faxes and telephone calls going into and out of the U.S. The fear is that data collection systems used by the NSA are not just monitoring suspected terrorists, but also filtering through the communications of potentially all ordinary law-abiding citizens.

Language of the Anti-Terrorism Act

“What is even more startling is that Canadian security agencies have been authorized to do the same thing here, and may be using the same approach to conduct vast data-mining of our communications ... the new Act allows it to spy on domestic communication, as long as it involves someone outside of Canada. The language of the legislation [Anti-Terrorism Act] mirrors that of the NSA mandate.”

— Warren Allmand,
Canadians need answers on domestic spying powers,
Toronto Star,
September 4, 2013.

http://www.thestar.com/opinion/commentary/2013/09/04/canadians_need_answers_on_domestic_spying_powers.html

Privacy is an Enshrined Right

“The right to privacy of one’s communications is a freedom that has been won after centuries of struggle in western democracies. This right is enshrined in our Charter of Rights and Freedoms, and in the International Covenant on Civil and Political Rights ratified by Canada in 1976.”

— Warren Allmand,
Canadians need answers on domestic spying powers,
Toronto Star,
September 4, 2013.

http://www.thestar.com/opinion/commentary/2013/09/04/canadians_need_answers_on_domestic_spying_powers.html

NSA has Cracked Most Online Encryption

- The U.S. National Security Agency is said to have secretly succeeded in breaking much of the encryption that keeps people's personal data safe online;
- This revelation emerged from documents leaked by former NSA contractor Edward Snowden to Britain's Guardian newspaper;
- According to the reports, the NSA, alongside its UK equivalent, Government Communications Headquarters, better known as GCHQ, has been able to unscramble much of the encoding that protects everything from personal e-mails to banking systems, medical records and Internet chats;
- The agencies' methods include the use of supercomputers to crack codes, covert measures to introduce weaknesses into encryption standards, and behind-doors collaboration with technology companies and Internet service providers.

— CNN,

Reports: NSA has cracked much online encryption,

September 6, 2013.

<http://www.cnn.com/2013/09/06/us/nsa-surveillance-encryption/>

Few See Adequate Limits on NSA Surveillance Program

- According to the Pew Research Institute, 47% say they are concerned that government anti-terrorism policies have gone too far in restricting the average person's civil liberties, while 35% say they are more concerned that policies have not gone far enough to protect the country;
- *This is the first time in Pew Research polling that more have expressed concern over civil liberties than protection from terrorism since the question was first asked in 2004.*

— Pew Research
July, 2103

<http://www.people-press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/>

We Need to Take the Internet Back

“To the engineers, I say this: we built the Internet, and some of us have helped to subvert it. Now, those of us who love liberty have to fix it.”

— Bruce Schneier,
The US government has betrayed the internet,
The Guardian,
September 5, 2013.

<http://www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-internet-nsa-spying>

Pew Internet Center Survey

- A Pew Internet Center survey conducted in July 2013, found that:
- 66% believed American laws were “not good enough in protecting their privacy online.”
- 55% were concerned about the breadth of personal information that exists about them online (a 22% increase from 2009).

Surveillance State Repeal Act

- Representative Rush D. Holt (D-N.J.) has proposed legislation that would prohibit the NSA from mandating that manufacturers install “back doors” to allow the government to bypass encryption. Representative Holt’s “Surveillance State Repeal Act” was introduced July 24, 2013.

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 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

New IPC White Paper

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 approach 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.



A Primer on Metadata: Separating Fact from Fiction

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

July 2013

*Introducing
A New Approach:
Applying Privacy by Design
to Surveillance*

www.privacybydesign.ca

What is Needed:

***Privacy-Protective Surveillance,
by Design***

Ann Cavoukian, Ph.D.

**Information and Privacy Commissioner of Ontario, Canada
and**

Khaled el Emam, Ph.D., et al.

**Associate Professor at the University of Ottawa,
Canada Research Chair Electronic Health Information**

Introducing PPS: Privacy-Protective Surveillance

- PPS only collects data that is considered to be “significant;”
- Significant data is defined by transactions or events that are believed to be related to suspicious activity;
- All personally identifiable information related to significant data will be encrypted;
- Analytics and queries will only be performed on encrypted data;
- If an interesting result is obtained, a more targeted request for the raw data that pertains to those results may be made;
- PPS is “blind” to data associated with unrelated events – it cannot “see” any other information;
- This avoids exposing the personal information of millions of people who are not considered to be persons of interest – leaving their privacy intact, and dramatically reducing the incidence of false positives.

The Underlying Technology – PPS

- PPS builds on “homomorphic” encryption and efficient protocols;
- These protocols require a semi-trusted third party – the key holder;
- Neither the key holder nor the data user can gain access to any raw identifiable data;
- A warrant or court order is required to decrypt data of interest.

Homomorphic Encryption

- A form of encryption that allows computations to be carried out on encrypted data, leading to encrypted results;
- “Homomorphic” describes the transformation of one dataset into another, while preserving relationships between data elements in both sets;
- Homomorphic encryption allows you to make computations or engage in data analytics on encrypted values – data you cannot “read” because it is not in plain text, therefore inaccessible;
- May also be used to link two or more databases without the disclosure of any unique identifiers – positive-sum – win/win;
Privacy by Design.



***A Preview of PPS:
Privacy-Protective
Feature Detection***

www.privacybydesign.ca

Objectives of PPS Feature Detection

- The ability to scan the Web and related databases using virtual agents to find digital evidence relating to potentially suspicious criminal activity by certain parties, without infringing the privacy of unrelated individuals;
- A technological infrastructure to ensure that the personally identifiable information (PII) of unsuspected individuals is not collected or retained and, for those associated with the targeted activity, PII may only be accessed with judicial authorization (a warrant).

What is a Feature?

A specific type of information or data correlation which, when combined with other features, may indicate suspicious behavior that would *warrant* further investigation.

Examples of Features

- FD1: Purchasing fertilizer capable of bomb-making;
- FD2: Accessing a bomb-making website;
- FD3: Transferring money to a “listed” organization;
- FD4: Telephone call to a “listed” individual;
- FD5: Telephone call from a “listed” telephone number.
- FDn: ...

What Will Be Stored if a Feature is Detected?

- The **fact** of a feature being detected, and only data related to that feature – a feature detector is in effect “**blind**” to anything other than the feature it was designed to detect – it is blind to “seeing” any other data;
- Once a feature is detected, any corresponding personally identifiable information will be encrypted along with the appropriate context, and only decrypted through a court order (a warrant).

Summary of PPS

- Privacy Protective Surveillance is a positive-sum, “win-win” alternative to current counter-terrorism surveillance systems. It incorporates two primary objectives in its design:
 1. the ability to scan the Web and related databases using a “blind-sight” procedure to detect digital evidence relating to potentially suspicious criminal/terrorist activity by some, without infringing on the privacy of unrelated individuals;
 2. a technological infrastructure to ensure that the personally identifying information (“PII”) on any unsuspected individuals is not collected and, in those associated with targeted activity, encrypted PII will only be divulged with judicial authorization (a warrant).

Concluding Thoughts

- Beware of the steady creep of surveillance technologies, expanding into an ever-growing number of mobile devices;
- Ensure that surveillance is accompanied by privacy measures embedded proactively by design, into IT systems and operational processes;
- Surveillance measures by the state must be subject to independent scrutiny, accompanied by prior judicial authorization and accountability measures;
- Let's 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**