

***Hands-On Privacy by Design:
A Working Session***

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

University of Alberta
2011 Access and Privacy Conference
June 16, 2011

The Decade of Privacy by Design



www.privacybydesign.ca

Privacy by Design: *The Trilogy of Applications*

**Information
Technology**

**Accountable
Business Practices**

**Physical Design
& Networked
Infrastructure**

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*):

Privacy by *ReDesign*

PbRD



Invitation to the first *PbD* *Privacy by ReDesign* Workshop

**33rd International Conference of Privacy
and Data Protection Commissioners**

November 1, 2011

Mexico City

www.privacyconference2011.org

www.facebook.com/cfpconf

Sponsored by American Express and Ernst & Young

www.privacybydesign.ca

Rethink, Redesign, and Revive: The 3 R's of *PbRD*

- ***Rethinking*** invites organizations to look at their risk mitigation strategies, legacy systems, and processes – including information technologies, business practices, physical design, and infrastructure – to consider using alternative approaches that are more privacy-protective. This may include revisiting assumptions about how much personal information is necessary for the system to operate: can you manage with less PII?;
- ***Redesigning*** represents the opportunity to enable or implement improvements in how the system functions from a privacy perspective, while also ensuring that it continues to achieve key business requirements in a positive-sum, win/win relationship;
- ***Reviving*** the system in a new, privacy-protective way is the ultimate goal – yielding new opportunities and avoiding the burden of costly data leakage.

PbRD Next Steps: Future Direction

- With *Privacy by Design* widely recognized as the new gold standard for the protection of personal information, there is a clear need for practical guidance as to how to accomplish its objectives and implement its principles:
 - American Express;
 - Ernst & Young;
 - ASU *Privacy by Design* Research Lab;
 - IBM;
 - *PbD*-PIA;
- I look forward to the participation of industry leaders and experts in the development of tools and resources such as Risk Management Frameworks, IT Security tools, Project Management instruments and best practices.

- Widespread Adoption of Mobile Communications Technology;
- Privacy and Mobile Communications;
- Roadmap for *PbD* in the Mobile Communications Industry:
 - Device Manufacturers;
 - OS/Platform & Application Developers;
 - Network Providers.

**The Roadmap for *Privacy by Design*
in Mobile Communications:
A Practical Tool for Developers,
Service Providers, and Users**



December 2010

ASU
PRIVACY BY DESIGN RESEARCH LAB

i
Information and Privacy Commissioner,
Ontario, Canada

- **Bering Media** has built Privacy into IP Geolocation:
- Using a unique double-blind privacy architecture;
- With minimum-match thresholds/ Anti-inference algorithms;
- Dynamic IP address management;
- Persistent, permanent opt-out.

Redesigning IP Geolocation: Privacy by Design and Online Targeted Advertising



October 2010


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

With contributions from:

beringmedia 

Mobile/Smartphone Tracking

- **Transparency** – give users clear notice from the outset;
- **Consent** – make it user-centric – make privacy the default;
- **Anonymized data** – don't let it be linked back to identifiers;
- **Data Minimization** – don't collect more data than you need;
 - When consumers find out *after the fact* that their data is being tracked, it erodes confidence and trust;
 - This is why we need *Privacy by Design* – privacy controls embedded directly into the system, right from the outset ... otherwise you can end up with *Privacy by Disaster*.

Survey Results are in:

Consumers Say Privacy is a Bigger Concern than Security on Smartphones

- **Privacy concerns rank #1:** Most consumers expressed great concern about their data privacy, both when using smartphones in general, and when using mobile apps in particular;
- Consumers want more control over their data: **98%** of consumers expressed a strong desire for better controls over how their personal information is collected and used via mobile devices and apps;
- A significant majority (**77%**) of consumers don't want to share their location data with app owners/developers.

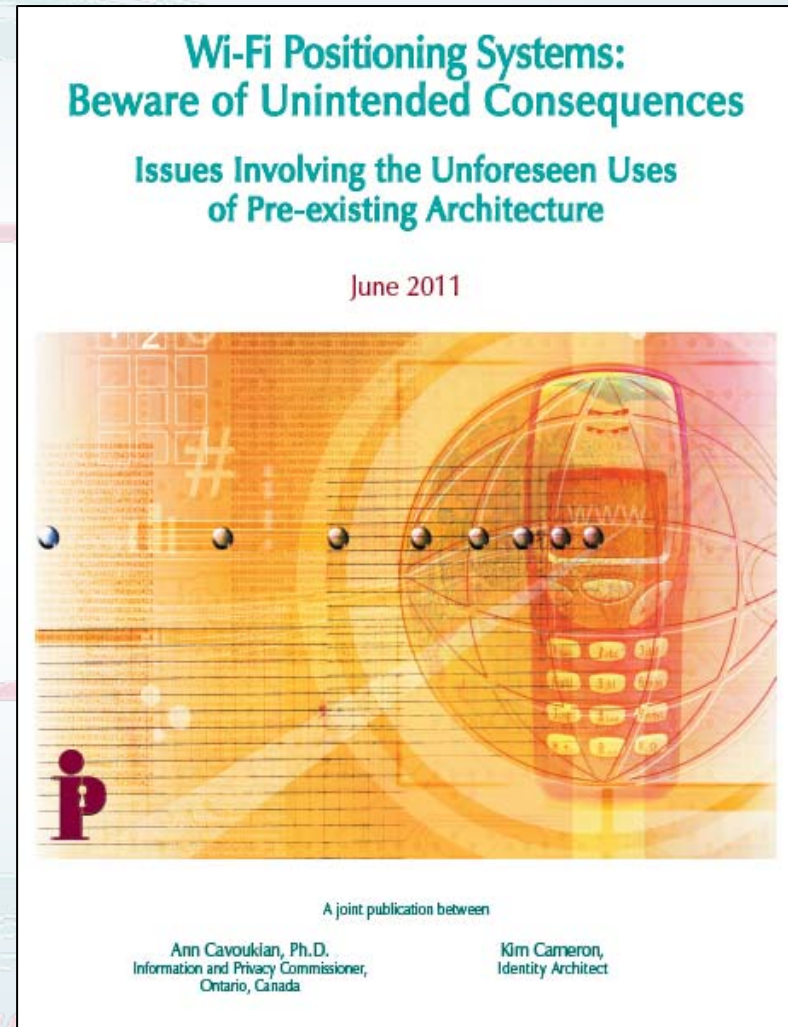
*Announcing Release
of New IPC Paper:*

**Wi-Fi Positioning Systems:
Beware of Unintended Consequences**

**Issues Involving the Unforeseen Uses
of Pre-existing Architecture**

Wi-Fi Positioning Systems: Beware of Unintended Consequences

- Advances in location-based technology and services;
- Overview of major positioning systems;
- Wi-Fi Positioning System “location aggregators;”
- *Privacy by Design*: Removing the “Informant” from WPS Location Architecture.



Unintended Consequence: “Unknowing Informant”

- Privacy concerns are raised whenever an individual uses location-based services because their mobile device can relay a unique identifier called a Media Access Control (MAC) address;
- The MAC address may be connected with other information about an individual such as physical location and lifestyle habits;
- Becoming an “unknowing informant” is an unintended consequence of building a location architecture using existing Wi-Fi networks which broadcast MAC addresses that are collected and geotagged;
- When designing an architecture (e.g. wireless networks), the question of unintended uses, inadvertently introduced through the existence of that architecture, should form part of a privacy threat risk analysis;
- *Privacy must be Designed* into Wi-Fi positioning systems to prevent “unintended consequences.”

“I encourage developers to participate and to keep Privacy by Design top of mind as they develop tools to allow users to take greater control of their information. If we want to preserve the privacy that so many of our freedoms rest upon, we need to commit to new and innovative approaches, and we need to do it now.”

— Commissioner Cavoukian



For Immediate Release: February 4, 2011

Contact:

Rebecca Farmer, ACLU of Northern California, 415.621.2493, rfarmer@aclunc.org

Doug Honig, ACLU of Washington, 206.624.2184, dhonig@aclu-wa.org

Andrew Lewman, The Tor Project, execdir@torproject.org

Angus Fisher, Ontario Information and Privacy Commissioner's Office, 416.326.3902, angus.fisher@ipc.on.ca

Privacy Groups Announce Developer Challenge for Mobile Apps

Competition Challenges Developers to Build Solutions for Mobile Privacy Concerns

Today four groups announced the 2011 Develop for Privacy Challenge (www.develop4privacy.org), a new competition for mobile application developers to address privacy concerns surrounding mobile phones and other portable devices. Sponsoring the Challenge are the ACLU of Northern California, the ACLU of Washington, and the Tor Project, with the assistance of the Ontario Information and Privacy Commissioner's Office. The winner will be announced in August 2011 at an event in Las Vegas, coinciding with the DEFCON and Black Hat security conferences.

By the end of 2011 the majority of cell phones sold in the U.S. will likely be smartphones that allow users to pull up maps, browse the Internet, check e-mail, and more. Roughly 50 million Americans already carry these devices. With all their convenience, smartphones can also collect and share vast amounts of data that can paint a detailed picture about someone's life: their current location, where they have been, who they know, what they search for online, and more. Unfortunately, the outdated federal law governing electronic privacy, the Electronic Communications Privacy Act (ECPA), was passed in 1986, long before smartphones or the Internet as we know it even existed.

"We shouldn't have to choose between using a smartphone and keeping our private information private," said Chris Conley, Technology and Civil Liberties Fellow at the ACLU of Northern California. "It's increasingly difficult for most people to understand where their data is going, let alone how they can reclaim control. Technology has evolved at breakneck speed, and although privacy laws don't auto-update, innovative developers can help fill the gap."

The 2011 Develop for Privacy Challenge is designed to address this imbalance by encouraging amateur and professional software developers to create tools that help mobile device users understand and address the privacy threats that all users face.

"We created the Develop for Privacy Challenge to call upon application developers to show that privacy doesn't need to be an afterthought in new technologies," said Brian Alseth, Technology and Liberty Director for the ACLU of Washington. "Rather, privacy can and should be a fundamental building block."

Applications submitted for the 2011 Develop for Privacy Challenge will be judged by a panel of leading privacy and technology experts, including Jacob Appelbaum of the Tor Project, Caspar Bowden of

Upcoming Event

PETs 2011

Privacy-Enhancing Technologies Symposium

July 27–29, 2011

Waterloo, Ontario, Canada

<http://petsymposium.org/2011/>

www.privacybydesign.ca

Ryerson University: Digital Media Zone

Digital Media Zone (DMZ) is a place where students, alumni, and companies can turn their innovations into market-ready products while seeking solutions to real-world, real-time problems

www.privacybydesign.ca

DMZ's Flybits: *The Embodiment of PbD*

- **Flybits** is a research team based at DMZ that focuses on ubiquitous and pervasive computing, with the goal of using mobile devices to enhance interpersonal communications – *while conserving privacy*.
- The ambient intelligence that is required for successful context-aware applications gives Flybits a mandate to develop *solutions for unique privacy problems*;
- Flybits is leading a project at Ryerson focused on building a **Privacy Rule Engine** for preserving user privacy in ubiquitous software applications,

<http://digitalmediazone.ryerson.ca/tag/flybits/>

Conclusions

- Lead with *Privacy by Design* and *Privacy by ReDesign*;
- Change the paradigm from the dated “zero-sum” to the doubly-enabling “positive-sum;”
- Deliver *both* privacy AND security or any other functionality, in an empowering “win-win” paradigm: abandon false trade-offs;
- Get rid of the “vs.” – replace it with “and;”
- Proactively embed privacy as a core functionality: deliver both privacy and security, not one to the exclusion of the other;
- Beware of unintended consequences!

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**