

Don't Sacrifice Privacy for Security: You Need Both – Privacy by Design

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

Presentation Outline

1. We Need to Change the Paradigm
2. *Privacy by Design*: The Gold Standard
3. Positive-Sum, NOT Zero-Sum
4. *Privacy by Design* Resolution
5. *New Extension: Privacy by ReDesign*
6. New Release: “*Wi-Fi Positioning Systems: Beware of Unintended Consequences*”
7. Conclusions

Setting the Stage:

Why We Need to

Change the Paradigm

The Future of Privacy

*Change the Paradigm to
Positive-Sum,
NOT
Zero-Sum*

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”***

What is Not Needed:

NOT

Privacy

vs.

Security

What is Needed:

Privacy

AND

Security,

not one,

to the exclusion of the other

A Matter of Balance?

The Trouble with “Balance” Metaphors

Julian Sanchez

www.juliansanchez.com

*Inspired by Orin Kerr’s paper on an
equilibrium-adjustment theory of the Fourth Amendment*

The Trouble with “Balance” Metaphors

“ ... the most obvious problem with balancing metaphors is that they suggest a relationship that is always, by necessity, zero sum: If one side rises, the other must fall, in exact proportion.”

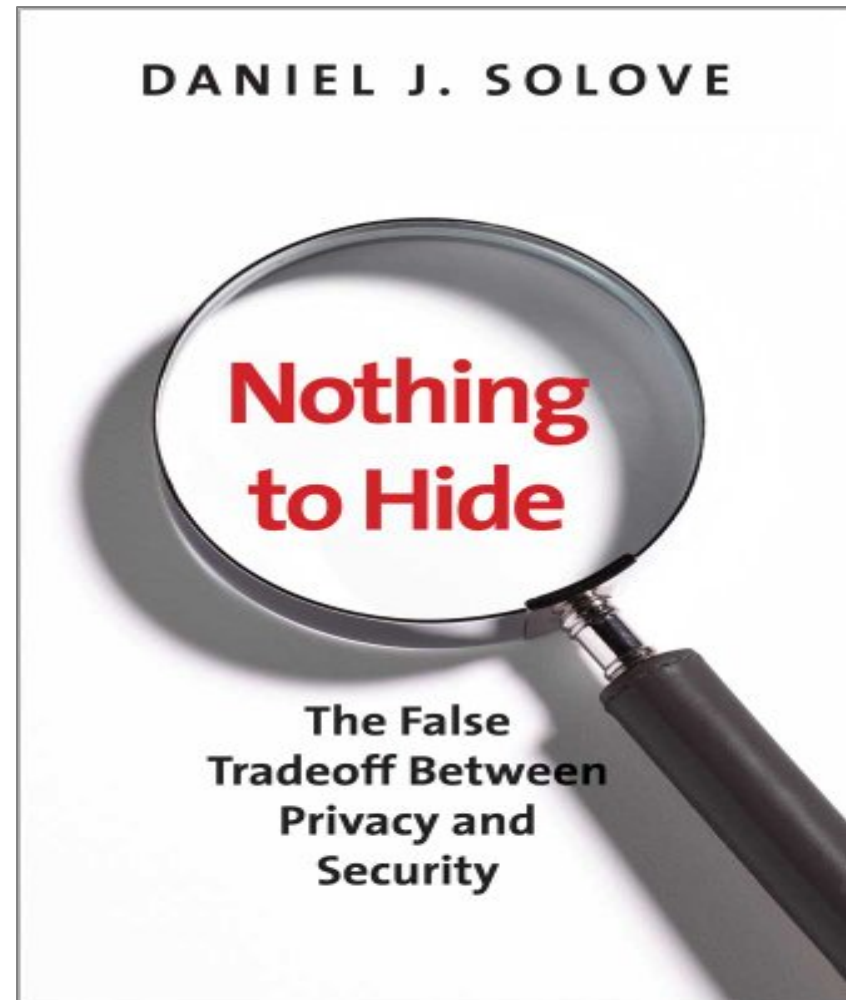
— Julian Sanchez, February 14, 2011.

www.juliansanchez.com

Nothing to Hide:

The False Tradeoff between Privacy and Security

“The debate between privacy and security has been framed incorrectly as a zero-sum game in which we are forced to choose between one value and the other. Why can't we have both?”



<http://docs.law.gwu.edu/facweb/dsolove/>

What Privacy is Not

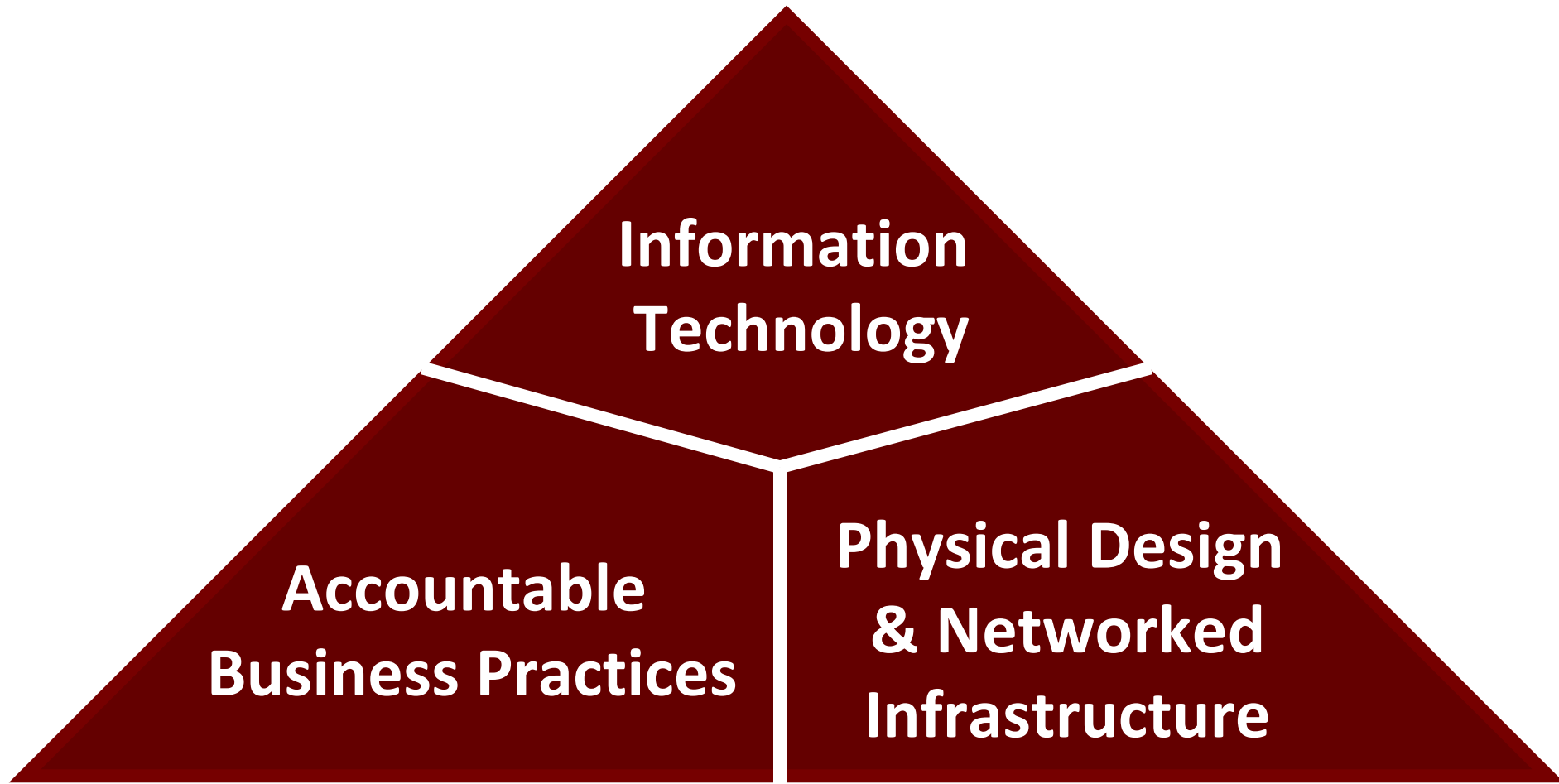
Privacy \neq Security

*Security is, however, vital to privacy:
You cannot have Privacy without Security*

The Decade of Privacy by Design



Privacy by Design: The Trilogy of Applications



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.



www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

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:

www.science20.com/newswire/landmark_resolution_passed_preserve_future_privacy

Privacy by Design in 2010: Gathering Momentum

- **May** – As part of the European Commission’s new European Digital Agenda, **Peter Hustinx**, the European Data Protection Supervisor, recommended that *Privacy by Design* be included as a binding principle into data protection legal framework;
www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf
- **October** – Regulators from around the world gathered at the annual assembly of **International Data Protection and Privacy Commissioners** in Jerusalem, Israel, and unanimously passed a landmark Resolution recognizing *Privacy by Design* as an essential component of fundamental privacy protection;
www.privacylaws.com/templates/EnewsPage.aspx?id=1663
- **December** – The **U.S. Federal Trade Commission** released a major report on protecting consumer privacy in which it recommended that companies adopt a *Privacy by Design* approach by building privacy protections into their everyday business practices.
www.privacybydesign.ca/media-centre/in-the-news/

Privacy by Design in 2011 ... We're Just Getting Started

- **February** – Debate in Dutch Senate began with a panel of experts deliberating data protection and privacy – consistently referring to the need for *Privacy by Design*, the first *PbD* certified consulting method for biometric identity systems being contemplated;
- **February** – Japan's Ministry of Economy, Trade and Industry translated the *Privacy by Design Foundational Principles* (on the heels of a Chinese translation), and is now replicating our *PbD* Ambassador Program in Japan;
- **April** – U.S. Senators John Kerry and John McCain cited *Privacy by Design* in their *Commercial Privacy Bill of Rights* that requires businesses that collect, use, store or transfer consumer information to implement data privacy protections when developing products and provide consumers with choices about how data are used, collected and shared.

Privacy by Design: Proactive in 21 Languages!

1.English

2.French

3.German

4.Italian

5.Spanish

6.Czech

7.Dutch

8.Estonian

9.Hebrew

10.Hindi

11.Chinese

12.Japanese

13.Arabic

14.Armenian

15.Korean

16.Ukrainian

17.Russian

18.Romanian

19.Portuguese

20.Maltese

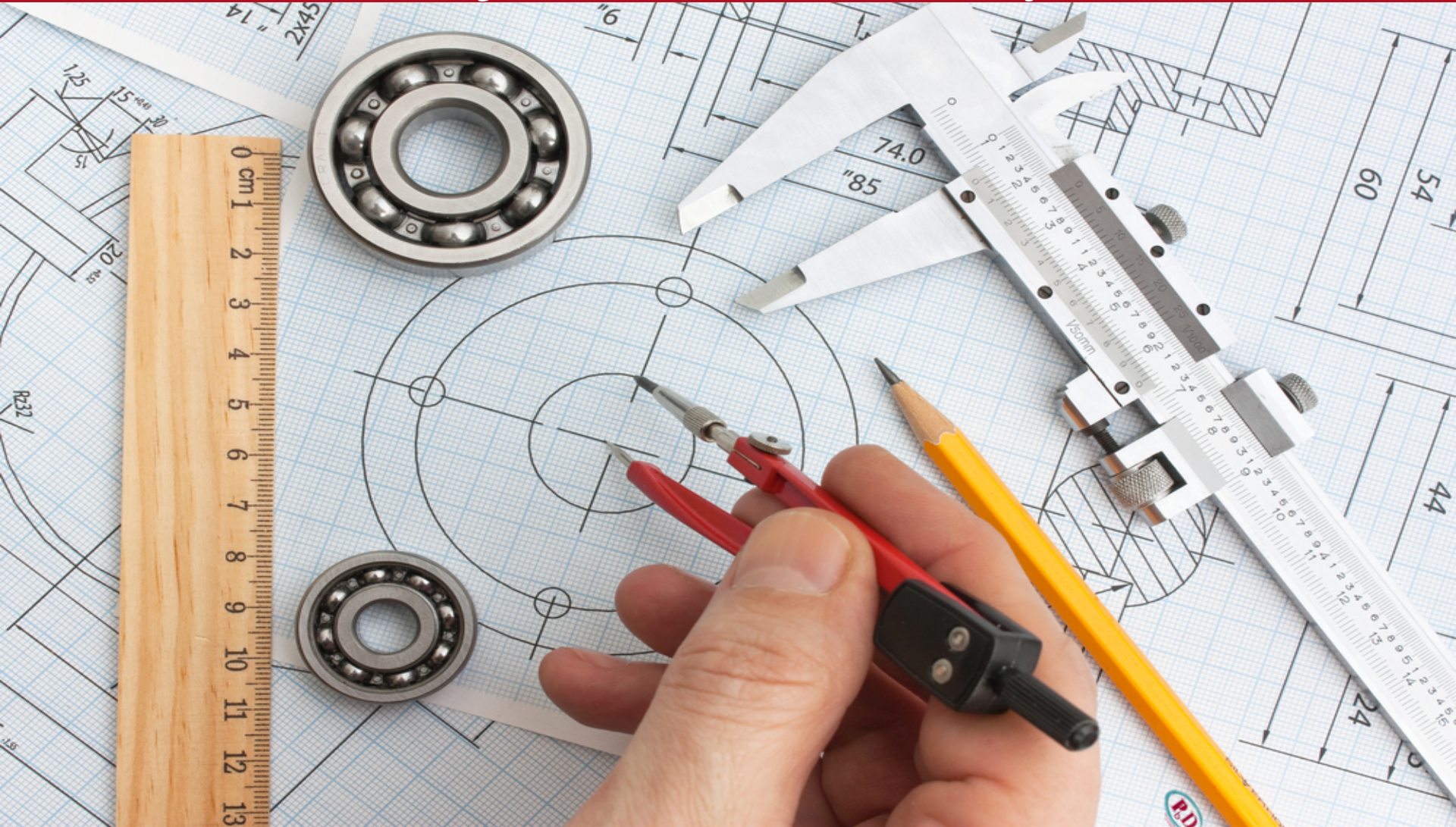
21.Greek

It Pays to be Proactive: Don't Wait for a Data Breach

*“... building privacy and security functions into a Smart Grid system AFTER it has been built costs **3 to 5 times as much.**”*

— Doug Westlund,
CEO of N-Dimension Solutions,
May 20, 2011

2011 – Year of the Engineer: *Beware of Unintended Consequences*



Mobile/Smartphone Tracking

- **Transparency** – give users clear notification 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*.

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

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 do 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.

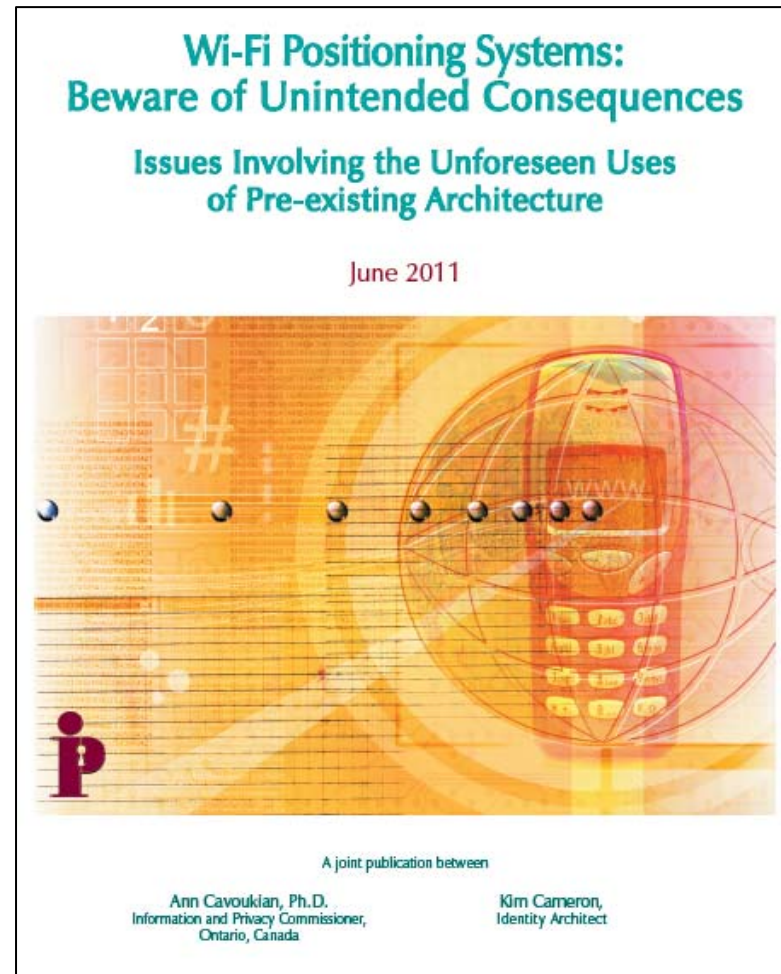
Announcing the Release of New White Paper:

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 Wi-Fi positioning systems;
- Wi-Fi Positioning System “location aggregators;”
- *Privacy by Design*: Removing the “Informant” from WPS Location Architecture.



www.privacybydesign.ca

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 wireless architecture, should form part of a privacy threat risk analysis;
- *Privacy **must** be Designed* into Wi-Fi positioning systems well before they are operational in order to prevent “unintended consequences.”

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;”
- 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