

“The Essential Need to Embed Privacy by Design into Smart Cities”

Ann Cavoukian, Ph.D.

Executive Director

Global Privacy & Security by Design Centre

Toronto, Canada

“The Essential Need to Embed Privacy by Design into Smart Cities”

Ann Cavoukian, Ph.D.

Executive Director

Global Privacy & Security by Design Centre

Toronto, Canada

MaRS Discovery District

Panel on Smart Cities

February 25, 2020

Let's Dispel The Myths

Privacy \neq Secrecy

Privacy is *not* about having
something to hide

Privacy = Control

Privacy = Personal Control

- User control is critical
- Freedom of choice
- Informational self-determination

Context is key!

Privacy is Essential to Freedom: A Necessary Condition for Societal Prosperity and Well-Being

- Innovation, creativity, and the resultant prosperity of a society requires freedom;
- Privacy is the essence of freedom: Without privacy, individual human rights, property rights and civil liberties – the conceptual engines of innovation and creativity, could not exist in a meaningful manner;
- **Surveillance is the antithesis of privacy:** A negative consequence of surveillance is the usurpation of a person's limited cognitive bandwidth, away from innovation and creativity.

The Decade of Privacy by Design



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

Why We Need *Privacy by Design*

Most privacy breaches remain undetected – as regulators, we only see the tip of the iceberg

The majority of privacy breaches remain unchallenged, unregulated ... unknown

Regulatory compliance alone, is unsustainable as the sole model for ensuring the future of privacy

Privacy by Design: Proactive in 40 Languages!

- | | | |
|---------------------|-----------------------|-----------------------|
| 1. <i>English</i> | 15. <i>Ukrainian</i> | 29. <i>Danish</i> |
| 2. <i>French</i> | 16. <i>Korean</i> | 30. <i>Hungarian</i> |
| 3. <i>German</i> | 17. <i>Russian</i> | 31. <i>Norwegian</i> |
| 4. <i>Spanish</i> | 18. <i>Romanian</i> | 32. <i>Serbian</i> |
| 5. <i>Italian</i> | 19. <i>Portuguese</i> | 33. <i>Lithuanian</i> |
| 6. <i>Czech</i> | 20. <i>Maltese</i> | 34. <i>Farsi</i> |
| 7. <i>Dutch</i> | 21. <i>Greek</i> | 35. <i>Finnish</i> |
| 8. <i>Estonian</i> | 22. <i>Macedonian</i> | 36. <i>Albanian</i> |
| 9. <i>Hebrew</i> | 23. <i>Bulgarian</i> | 37. <i>Catalan</i> |
| 10. <i>Hindi</i> | 24. <i>Croatian</i> | 38. <i>Georgian</i> |
| 11. <i>Chinese</i> | 25. <i>Polish</i> | 39. <i>Urdu</i> |
| 12. <i>Japanese</i> | 26. <i>Turkish</i> | 40. <i>Tamil</i> |
| 13. <i>Arabic</i> | 27. <i>Malaysian</i> | 41. <i>Afrikaans</i> |
| 14. <i>Armenian</i> | 28. <i>Indonesian</i> | (pending) |

Two Essentials to Privacy by Design

1. Prevent the harms from arising:
You must be Proactive!
2. Banish Zero-Sum Models!

**Get Rid of the Dated
Win/Lose, Zero-Sum Models!**

Positive-Sum Model: *The Power of “And”*

*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 “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**.



<http://www.ryerson.ca/pbdce/papers/>
<http://www.ontla.on.ca/library/repository/mon/24005/301946.pdf>

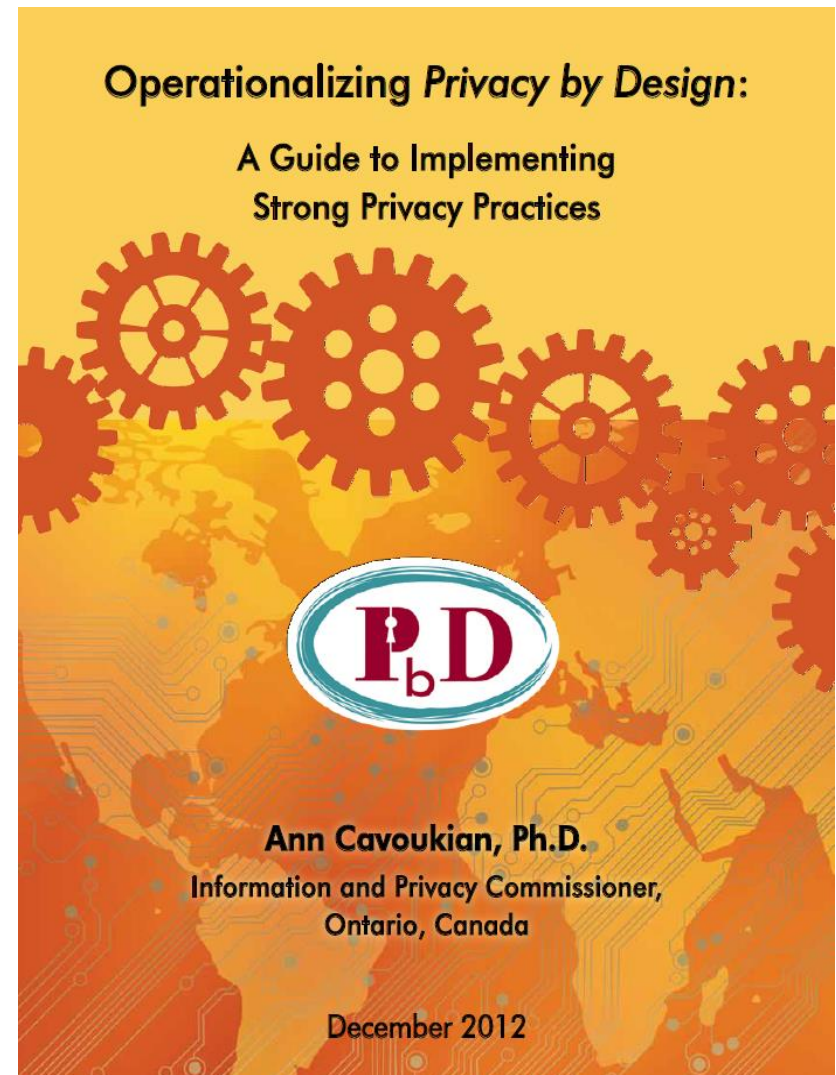
Operationalizing *Privacy by Design*

11 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;
- Privacy Protective Surveillance;
- SmartData.

<http://www.ryerson.ca/pbdce/papers/>

<http://www.ontla.on.ca/library/repository/mon/26012/320221.pdf>



Letter from JIPDEC – May 28, 2014

“Privacy by Design is considered one of the most important concepts by members of the Japanese Information Processing Development Center ...

We have heard from Japan’s private sector companies that we need to insist on the principle of Positive-Sum, not Zero-Sum and become enlightened with Privacy by Design.”

— Tamotsu Nomura,
Japan Information Processing Development Center,
May 28, 2014

Cost of Taking the Reactive Approach to Privacy Breaches

Proactive



**Class-Action
Lawsuits**

**Damage to
One's Brand**

Reactive



**Loss of Consumer Confidence
and Trust**

GDPR

General Data Protection Regulation

- Strengthens and unifies data protection for individuals within the European Union
 - Gives citizens control over their personal data and simplifies regulations across the EU by unifying regulations
-
- Proposed – January 25th 2012
 - Passed - December 17th, 2015
 - Adoption – Spring, 2016
 - Enforcement – May 25th, 2018

E.U. General Data Protection Regulation

- The language of “Privacy/Data Protection by Design” and “Privacy as the Default” will now be appearing for the first time in a privacy statute, that was recently passed in the E.U.
 - Privacy by Design
 - Data Protection by Design
 - Privacy as the Default

The Similarities Between PbD and the GDPR

“Developed by former Ont. Information & Privacy Commissioner, Ann Cavoukian, Privacy by Design has had a large influence on security experts, policy makers, and regulators ... The EU likes PbD ... it’s referenced heavily in Article 25, and in many other places in the new regulation. **It’s not too much of a stretch to say that if you implement PbD, you’ve mastered the GDPR.**”

Privacy Commissioner of Canada: Annual Report

“Organizations must also be more transparent and accountable for their privacy practices. Because they know their business best, it is only right that we expect them to find effective ways, within their own specific context, to protect the privacy of their clients, **notably by integrating approaches such as Privacy by Design.**”



HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

TOWARDS PRIVACY BY DESIGN: REVIEW OF THE *PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT*

**Report of the Standing Committee on Access to
Information, Privacy and Ethics**

Bob Zimmer, Chair

42nd Parliament, First Session
February, 2018

Privacy by Design Certification

**We have now re-launched
Privacy by Design Certification
lead by Dr. Ann Cavoukian,
partnering with KPMG**

www.ryerson.ca/pbdce/certification

“Privacy by Design – Ready for Takeoff”

“The passage of the EU’s GDPR ... is bringing PbD to top of mind as personal operations are adjusted to comply with new GDPR rules...In short, the GDPR has already given PbD new visibility and vigor. Positive-sum change is on its way – not just to Europe, but across the world.”

“Dr. Cavoukian is keeping up with change as well, having recently founded GPSbyDesign, A follow-up to PbD, now expanded to a global privacy and security focus. PrivacyCheq supports GPSbyDesign, and works to promote its acceptance.”

Global Privacy and Security Experts Launch the International Council on Global Privacy and Security, by Design

New organization created to educate governments and businesses on how to develop policies and technologies where privacy, public safety and Big Data work together for positive-sum, win-win outcomes

Founding Members include:

- Darren Entwistle, CEO of TELUS Inc.
- Michael Chertoff, 2nd Secretary of U.S. Homeland Security
- Gilles de Kerchove, Director of E.U. Counter Terrorism
- Greg Wolfond, CEO of SecureKey
- Joseph Simitian, Supervisor of Santa Clara County, CA and Former Chair of the California State Senate Select Committee on Privacy

Press Release: <http://m.marketwired.com/press-release/-2167023.htm>


International Council on Global Privacy and Security, by Design

- Newly created extension of Privacy by Design, focusing on both Privacy and security!
- Essential need to abandon zero-sum, either/or propositions involving one interest vs. another: privacy vs. public safety;
- Change this to a doubly-enabling positive-sum approach, with both privacy AND public safety gaining in positive increments.

www.gpsbydesign.org

Privacy by Design: The Global Privacy Framework

Dr. Cavoukian is offering the definitive
Privacy by Design Online Course
at Ryerson University



Enrol today

Privacy by Design (CZLW 327)
Develop the skills necessary to embed privacy into the design of your organization's information technology infrastructure and business practices.

**Offered online by
Dr. Ann Cavoukian**

Ryerson University | The Chang School of Continuing Education

<https://www.ryerson.ca/pbdce/privacy-by-design-chang-school-course/>

Smart Cities

The Essential Need to Embed
Privacy by Design into
Smart Cities

An Example of the need for “De-Identified at Source”: Smart Cities

Smart City Privacy – Potential Challenges as Our Cities Become More Connected

“Sensors are becoming cheaper, wireless connectivity is becoming ubiquitous, and computing power continues to increase. An incredibly connected world and smart cities are going to be a reality. It’s a question of when, not if.”

Calum McClelland,
IoT For All,
November 26th, 2016

<https://www.iotforall.com/smart-city-privacy/>

**Personal Data
Must be De-Identified,
at Source**

Smart Cities

- Non-stop sensors and emerging technologies will be “on” 24/7;
- There will be no opportunity for residents to consent or revoke consent.

**If data are not
de-identified at source,
right at the time when
the data are collected,
we will inevitably create
Smart Cities of Surveillance**

**Let's create
Smart Cities of Privacy!
Privacy must be preserved
if we wish to preserve
our freedoms**

Waterfront Toronto Smart City

“... a lot of issues around privacy can be addressed by anonymizing data right from the beginning.”

“All of the personally identifiable information that could be collected here needs to be de-identified and delinked from the broader data sets, so that you don’t run into a situation where there’s a bit of a surveillance city ... **it should be a neighbourhood that’s really grounded in privacy.**”

Kristina Verner,
VP of Innovation,
Sustainability and Prosperity,
Waterfront Toronto
January 30th, 2019
Financial Post

<https://business.financialpost.com/technology/smart-cities-may-be-too-smart-for-their-own-good>

International Council of Smart Cities

Privacy in Smart Cities

Study Period Report

Use cases identified:

- Platform for Citizen Engagement
- Traffic Mobile App
- CCTV Surveillance
- Wifi-IT Connectivity
- Virtual Hospital
- Smart Grid and Energy

Udbhav Tiwari
Antonio Kung
ISO/IEC JTC SC 27 Meetings
April 19, 2017

Privacy in Smart Cities (cont'd.)

Data Life Cycle:

- Collection - Interpreted, aggregated, filtered and analysed correctly.
- Storage/Retention - Retain important data elements, delete unnecessary.
- Use - Degree of collection, private control, big data implications.
- Transfer - Affordable, uninterrupted, high speed and interoperable.
- Deletion - Effective data governance balanced with feasibility, legal requirements.
- Security - Standards for cyber security testing, data breaches.
- Transparency - Need for citizens to observe and interact for accountability.

Udbhav Tiwari
Antonio Kung
ISO/IEC JTC SC 27 Meetings
April 19, 2017

Privacy in Smart Cities (cont'd.)

Privacy Controls:

- Data Ownership
- Communication channels
- Compute
- Storage
- Reporting
- General authority for “Subjects”
- Insurance

Udbhav Tiwari
Antonio Kung
ISO/IEC JTC SC 27 Meetings
April 19, 2017

Concluding Thoughts

- Privacy and security risks are best managed by proactively embedding the principles of *Privacy by Design* – prevent the harm from arising – avoid the data breach;
- Focus on prevention: It is much easier and far more cost-effective to build in privacy and security, up-front, rather than after-the-fact , reflecting the most ethical treatment of personal data;
- Abandon zero-sum thinking – embrace doubly-enabling systems: Privacy and Security; Privacy and Data Utility;
- Get smart – lead with *Privacy by Design*, not privacy by chance or, worse, *Privacy by Disaster*!

Contact Information

Ann Cavoukian, Ph.D., LL.D (Hon.) M.S.M.
Executive Director
Global Privacy & Security by Design Centre

Phone: (416) 357-2818

ann.cavoukian@gpsbydesigncentre.com



ann.cavoukian@gpsbydesigncentre.c
om



twitter.com/AnnCavoukian