

Privacy and Security by Design: Regulatory Compliance Will Not be Enough to Preserve our Privacy

Ann Cavoukian, Ph.D.

**Distinguished Expert-in-Residence
Privacy by Design Centre of Excellence
Ryerson University**

**Ryerson CSR Institute / PPOCIR
Privacy Protection in 2018
December 7th, 2018**

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.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

32.Serbian

33.Lithuanian

34.Farsi

35.Finnish

36.Albanian

37.Catalan

38. Georgian

39. Urdu

40. Tamil

41. Afrikaans

(pending)

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>

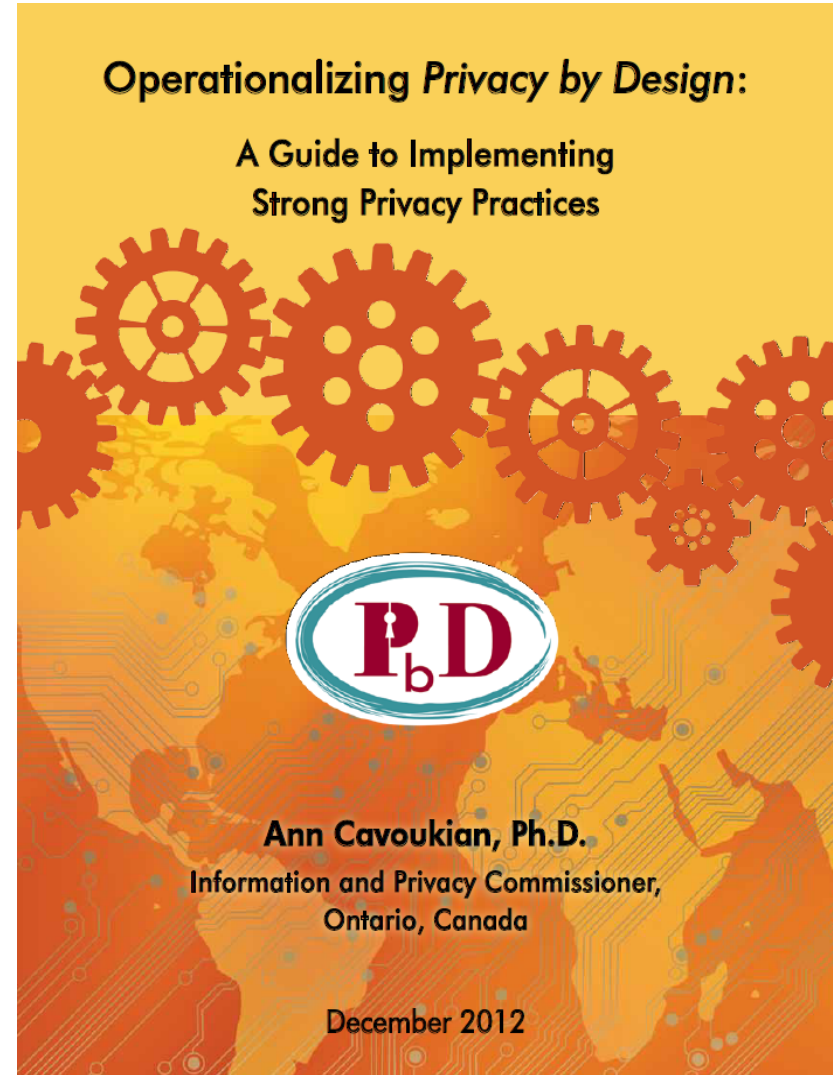
Operationalizing *Privacy by Design*

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

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 17, 2015
 - Adoption – Spring 2016
 - Enforcement – Spring 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.**”

Information Age
September 24, 2015

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.**”

September 21, 2017

https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/#heading-0-0-3-1

RYERSON
UNIVERSITY



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

<https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9690701/ethirp12/ethirp12-e.pdf>

**RYERSON
UNIVERSITY**

Privacy by Design as an ISO Standard

- New ISO Project Committee on Privacy by Design for Consumer Goods and Services (ISO PC317);
- The Standards Council of Canada (SCC) is the mirror committee for the International PC 317 committee.

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](http://www.ryerson.ca/pbdce/certification)

Privacy by Design Certification

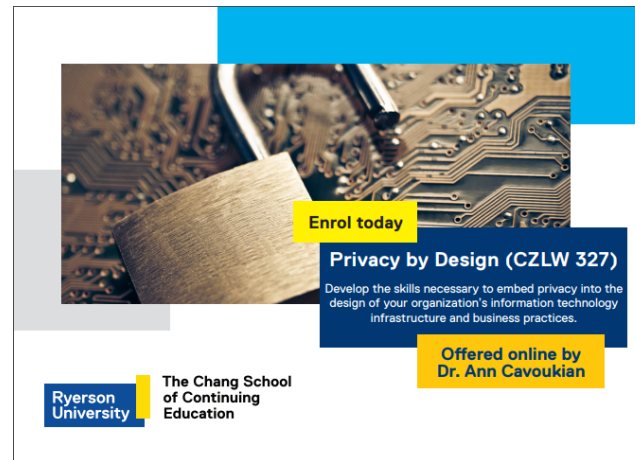
- We chose to partner with Sylvia Kingsmill, Senior Partner at KPMG, for our re-launch of Privacy by Design Certification, to ensure that our upgraded Certification seal provides proof of compliance with the GDPR;
- We have also aligned with ISO, a leading accredited certification body, in our international re-launch of Privacy by Design Certification.

Canadian Companies Have Taken the Lead with PbD Certification

- Leading companies have taken a proactive risk management approach to protecting their customers' privacy by getting certified, as opposed to doing the least required via regulatory compliance;
- At a time when trust is at an all-time low, and data breaches are proliferating, companies realize that in getting certified, it's a reputational exercise to enhance one's brand, not a "tick-the-box" compliance exercise.

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

Should you wish to sign up for the Fall 2018 registration list, visit:
<https://www.ryerson.ca/pbdce/privacy-by-design-chang-school-course/>

Privacy: The Business Case

***Privacy is
Good for Business!***

The Bottom Line

Privacy should be viewed as a
business issue, not a
compliance issue

*Think strategically and transform privacy into a
competitive business advantage*

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**

First “Privacy Marketplace” at the International Consumer Electronics Show in Vegas

*“ Privacy is a hot issue right now. It’s on everyone’s radar ... Consumers asking about privacy – that was the big takeaway. These companies in the privacy marketplace, in large part aren’t advocates. They’re **entrepreneurs** looking to capitalize on market opportunity. They expect a larger privacy marketplace next year **and for brands to incorporate “privacy” into their marketing...** Anyone, everyone, can understand the need for privacy.”*

Victor Cocchia
CEO, Vysk

Speaking at CES: Jan 2015

Guard Your Reputation

**“Trust takes years to build,
seconds to destroy, and forever
to repair.”**

**... And trust among the public is at
an all-time low today**

Pew Research Internet Project

- **Public Perceptions of Privacy and Security in the Post-Snowden Era: November 2014**
 - There is widespread concern about surveillance by both government and business:
 - **91% of adults agree that consumers have lost control over their personal information;**
 - 80% of social network users are concerned about third parties accessing their data;
 - 80% of adults agree that Americans should be concerned about government surveillance;

The Online “Privacy Lie” Is Unraveling

Joseph Turow and Michael Hennessy, University of Pennsylvania
Nora Draper, University of New Hampshire

“A large majority of web users are not at all happy ... they feel powerless to stop their data being harvested and used by marketers.”

91% disagree that “If companies give me a discount, it is a fair exchange for them to collect information about me without my knowing.”

June 6, 2015

TechCrunch

<http://techcrunch.com/2015/06/06/the-online-privacy-lie-is-unraveling/>

2014 Survey of Canadians on Privacy

Office of the Privacy Commissioner of Canada

- **90% of Canadians expressed concern about the protection of their privacy;**
- 78% feel at least somewhat likely that their privacy may be breached by someone using their Credit/Debit Card or stealing their identity;
- 70% of Canadians are concerned about the use of genetic testing for non-medical purposes;
- 73% feel they have less protection of their personal information than ten years ago;
- 60% have little expectation of privacy because there are so many ways it can be compromised.

Trends and Challenges: *Consumer Confidence*

- People choose to give their business to firms with good “**data hygiene**” – new evidence suggests that consumers are seeking out companies that will protect their privacy.

— Forrester Research

Privacy and Marketing

“Privacy by Design Is a Starting Point That Leads to Long-Term Benefits”

Jessica Kernan
Advertising Age
Oct, 28 2014

“By adopting a privacy-by-design mentality, we can begin to transform ideas like these into best practices that have long-term benefits for both consumers and brands.

Let's lead the way.”

Jessica Kernan
Advertising Age
Oct, 28 2014

Three Key Points to Help Marketers:

1. Integrate data planning as an upstream design discipline;
2. Evolve from fine print to more transparent disclosure strategies;
3. Make Privacy a positive part of the brand experience.

Jessica Kernan
Advertising Age
Oct, 28 2014

10 Take-Aways from Dr. Cavoukian's Talk

- Privacy is not about secrecy, it's about control.
- Many believe you can either have privacy *or* security, but security and privacy can co-exist.
- Six out of 10 Americans are distrustful of their government.
- Zero-sum thinking will only hold you back. Embrace doubly-enabling systems: marketing *and* privacy.
- Focus on integrating data planning as an upstream design discipline.
- Evolve from fine print to more transparent disclosure strategies.
- Make privacy a positive part of the brand experience.
- Increase consumer trust right out of the gates. Privacy can be your competitive advantage.
- Be deliberate and proactive: lead with *Privacy by Design* rather than privacy by chance.
- Privacy is good for business!

The Unintended Consequences of Data

“ The increasing availability of ‘data fumes’ – data produced as a by-product of **people’s use of technological devices and services** – has both political and practical implications for the way people are seen and treated by the state and by the private sector.”

Linnet Taylor,
TILT, Tilburg University
February 16, 2017

IoT Attacks: “When” not “IF”

“The question companies should be asking is no longer whether there will be an attack involving Internet of Things (IoT) devices and infrastructure, but when.”

Hogan Lovells
HL Chronicle of
Data Protection
May 8, 2017

Security Deserves Far Greater Attention

- Cyber Security threats are mounting on a daily basis;
- And they are also leading to massive lawsuits – class action lawsuits.

1.1 Billion Identities Stolen in 2016

IAPP, April 26, 2017

Data Breach Statistics

Data records lost or stolen
since 2013:

9,053,156,308

Breach Level Index,
2017

<http://breachlevelindex.com/>

Data Breach Statistics (cont'd)

Only 4%

of breaches were “Secure Breaches”
where encryption was used and the stolen
data was rendered useless.

The Vital Need for Encryption!

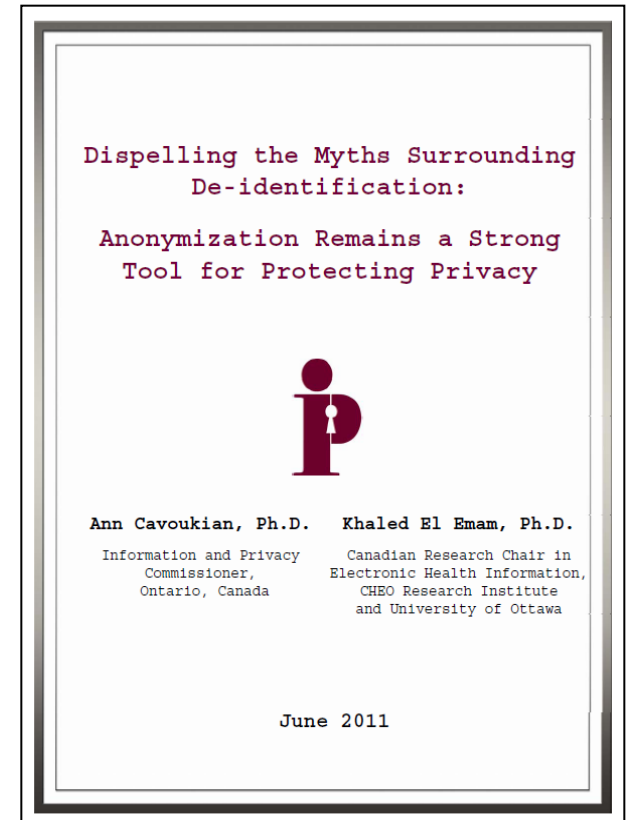
Data Minimization and De-Identification

Data Minimization

- Data minimization is the most important safeguard in protecting personally identifiable information, including for a variety of research purposes and data analysis;
- The use of strong de-identification techniques, data aggregation and encryption techniques, are absolutely critical.

Dispelling the Myths about De-Identification...

- The claim that de-identification has no value in protecting privacy due to the ease of re-identification, is a **myth**;
- If proper de-identification techniques and re-identification risk management procedures are used, re-identification becomes a very difficult task;
- While there may be a residual risk of re-identification, in the vast majority of cases, de-identification will strongly protect the privacy of individuals when additional safeguards are in place.



www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1084

Essential Need for strong De-Identification

- Personally identifiable data must be rendered non-identifiable, thereby enabling use of data for research purposes;
- Strong de-identification protocols must be used in conjunction with a risk of re-identification framework.

The Myth of Zero-Risk

5 Standards on De-Identification, Taking a Risk-Based Approach, Cont'd.

1. Institute of Medicine:

Sharing Clinical Trial Data: Maximizing Benefits, Minimizing Risk
Committee on Strategies for Responsible Sharing of Clinical Trial Data

2. HI Trust: Health Information Trust Alliance:

De-Identification Framework:

A Consistent, Managed Methodology for the De-Identification of Personal Data and
the Sharing of Compliance and Risk Information

5 Standards on De-Identification, Taking a Risk-Based Approach, Cont'd.

3. Council of Canadian Academies:

Accessing Health and Health-Related Data in Canada

The Expert Panel on Timely Access to Health and Social Data for Health Research and Health System Innovation

4. PhUSE Pharmaceutical Users Software Exchange:

De-Identification Standard for CDISC SDTM 3.2

PhUSE De-Identification Working Group

5. NISTIR 8053 De-Identification of Personal Information

National Institute of Standards and Technology

Risk Mitigation Strategies

“Boards really want to understand the operational risk to their company, along with the plans for how one wants to handle risk and reduce the impact.”

-Jim Anderson
BAE Systems Applied Intelligence

Do you have a Data Map?

- Do you know how personally identifiable data flows throughout your organization?
- Do you know if the necessary permissions have been obtained?
- Do you know if the data flows outside your organization to third parties? (authorized or not)
- Do you have a risk mitigation strategy?

Privacy Impact Assessments (Intended to be an Analytical Process)

“The goal of a PIA is to identify and address privacy risks when planning, designing, acquiring and implementing new programs, systems, processes, practices, services, technology, applications that involve personal information.”

Eric Lawton,
Privacy and Access Council of Canada,

Data Breach Response

- Do you have a **Data Breach Protocol** in place, that kicks in the minute you get a data breach?
- Have all your staff been trained to follow the protocol?
- Do they know exactly what to do as soon as they are alerted of a data breach?

“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.”

Privacy Elephant
November 4, 2016

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.

gpsbydesign.org

My Resignation from Sidewalk Labs

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 Certification*, not privacy by chance or, worse, *Privacy by Disaster!*

Contact Information

Ann Cavoukian, Ph.D., LL.D (Hon.) M.S.M.
Distinguished Expert-in-Residence
Privacy by Design Centre of Excellence
Ryerson University

1 Dundas St. West, 25th Floor
Toronto, Ontario
M5G 1Z3

Phone: (416) 979-5000 ext. 553138

ann.cavoukian@ryerson.ca



ann.cavoukian@ryerson.ca



twitter.com/AnnCavoukian