

# **Don't Think of Privacy as a Barrier: Health Data Deserves the Strongest Protection**

**Ann Cavoukian, Ph.D.**

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

**Drug Pricing Policy Summit:  
Patients Redefining Healthcare  
November 13<sup>th</sup> -14<sup>th</sup>, 2018**

# Let's Dispel The Myths

# Privacy $\neq$ Secrecy

Privacy is *not* about having something to hide

# Privacy = Control

# Privacy = Personal Control

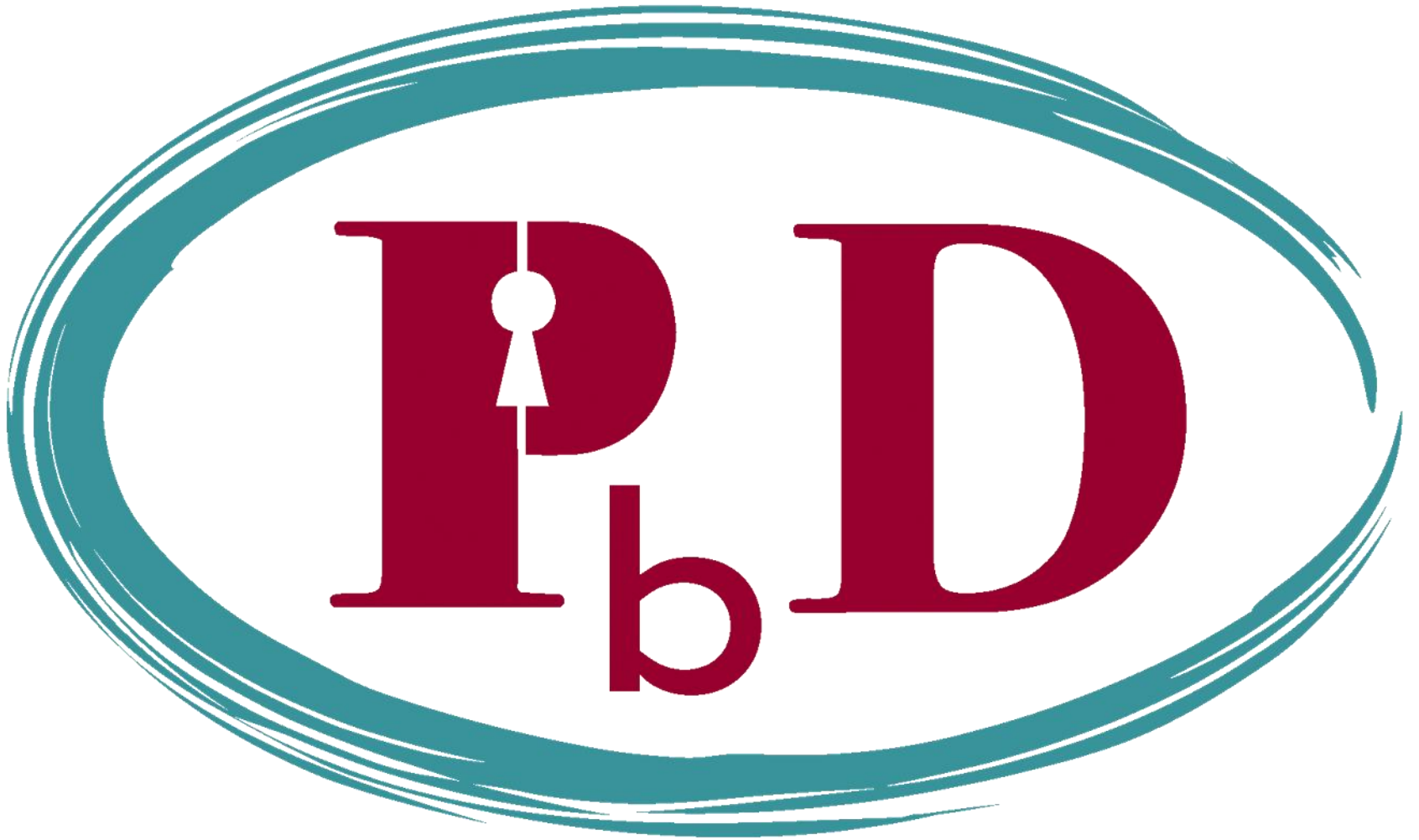
- User control is critical
- Freedom of choice
- Informational self-determination

**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](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](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)             |

# 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>



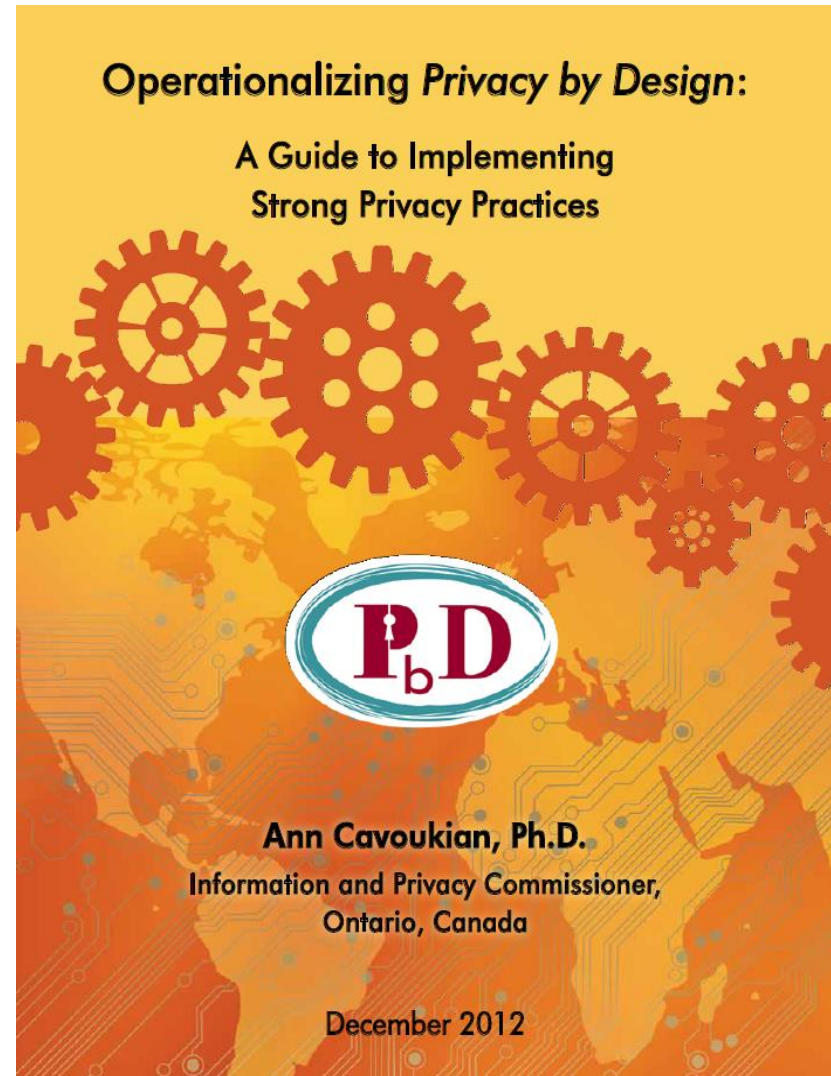
# Operationalizing *Privacy by Design*

## 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 25<sup>th</sup> 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

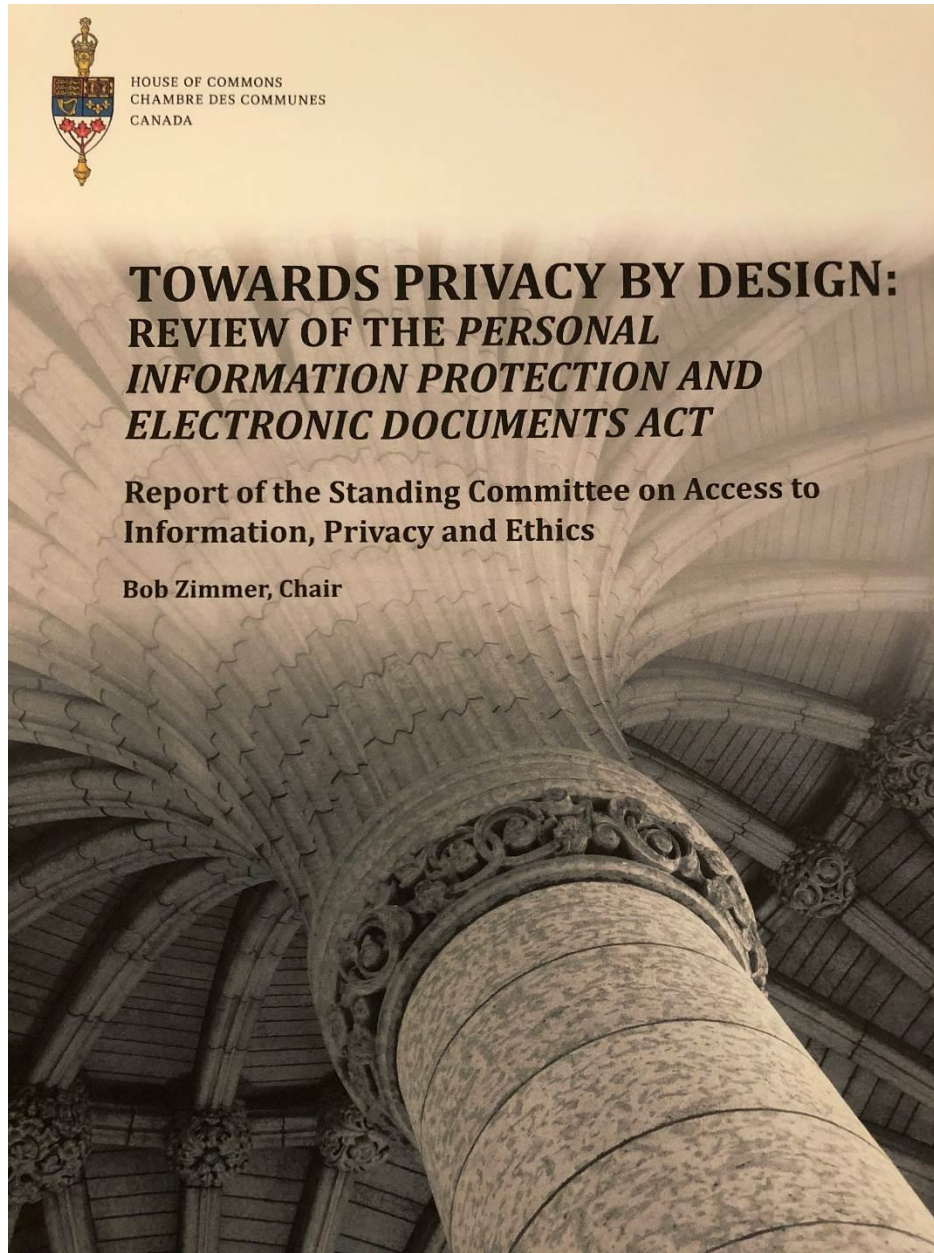


HOUSE OF COMMONS  
CHAMBRE DES COMMUNES  
CANADA

# **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**



42<sup>nd</sup> Parliament, First Session  
February, 2018

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

RYERSON  
UNIVERSITY

# 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)**

# **Ontario's Personal Health Information Protection Act (PHIPA)**

# PHIPA – The Gold Standard

- *PHIPA* serves as a model for other health privacy statutes;
- The New Brunswick Task Force on Personal Health Information regards *PHIPA* “as the gold standard among personal health information privacy statutes in Canada”;
- The U.S. Institute of Medicine recommended that *PHIPA* be used as the model to amend its health privacy statute, the *Health Insurance Portability and Accountability Act*.

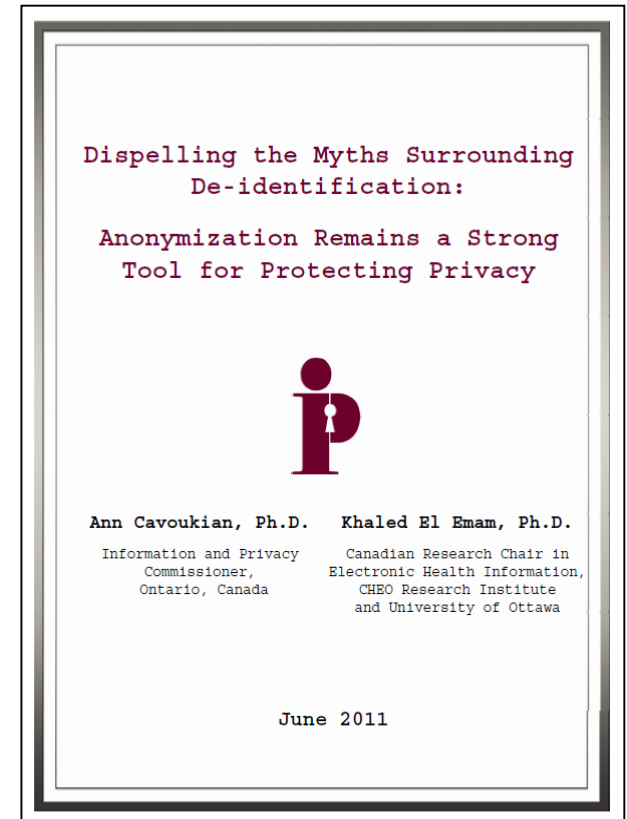
# ***Data Minimization and De-Identification***

# 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](http://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;
- Strong de-identification protocols must be used in conjunction with a risk of re-identification framework.

# Research Ethics by Design: A Collaborative Research Design Proposal

**Dr. Donald S Borrett**

Michael Garron Hospital, Toronto East Health Network

**Dr. Heather Sampson**

Michael Garron Hospital, Toronto East Health Network

**Dr. Ann Cavoukian**

Privacy by Design Centre of Excellence, Ryerson University

<http://journals.sagepub.com/doi/pdf/10.1177/1747016116673135>

# Research Ethics by Design

Privacy by Design, advances the view that privacy cannot be assured solely by compliance with regulatory frameworks but must become an organisation's default mode of operation. We are proposing a similar template for the research ethics review process. **The Research Ethics by Design framework involves research ethics committees engaging researchers during the design phase of the proposal so that ethical considerations may be directly embedded into the science, as opposed to being viewed as addendums, after the fact.** This results in the establishment of a culture of ethical research rather than research with ethical oversight.

# The Myth of Zero-Risk

# 5 Standards on De-Identification: Taking a Risk-Based Approach

## 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, 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

# Innovate with De-Identified Data

- De-Identification and data minimization are among the most important safeguards in protecting personal information;
- You should not collect, use or disclose personal information if other data (i.e., de-identified, encrypted or obfuscated) will serve the purpose;
- The use of strong de-identification, aggregation, and encryption techniques are absolutely critical, and readily available.

*“There are considerable risks in abandoning de-identification efforts, including the fact that individuals and organizations may simply cease disclosing de-identified information for secondary purposes, even those seen to be in the public interest.”*

— Commissioner Cavoukian

## **De-identification Protocols: Essential for Protecting Privacy**



June 25, 2014

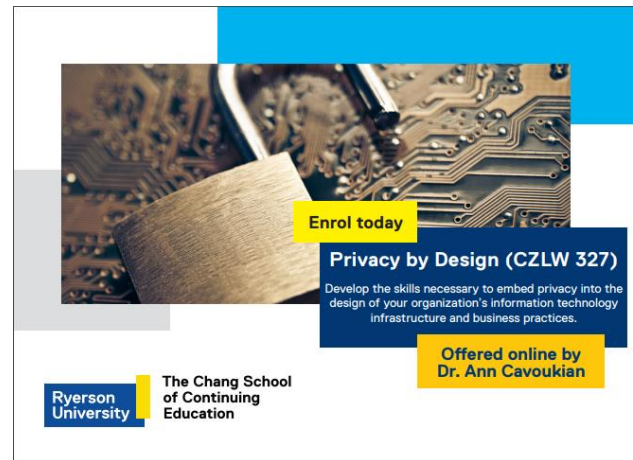
**Ann Cavoukian, Ph.D.**  
Information and Privacy Commissioner  
Ontario, Canada

**Khaled El Emam, Ph.D.**  
Canada Research Chair  
in Electronic Health Information  
University of Ottawa



# 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/>

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

1 Dundas St. West, 25<sup>th</sup> Floor  
Toronto, Ontario  
M5G 1Z3

Phone: (416) 979-5000 ext. 553138

[ann.cavoukian@ryerson.ca](mailto:ann.cavoukian@ryerson.ca)



[ann.cavoukian@ryerson.ca](mailto:ann.cavoukian@ryerson.ca)



[twitter.com/AnnCavoukian](https://twitter.com/AnnCavoukian)