

The Essential Need to Embed Privacy and Security, by Design

Ann Cavoukian, Ph.D.

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

Reboot 20th Privacy & Security Conference
February 6th- 8th, 2019
Victoria, BC

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.

“They Know Everything About You”

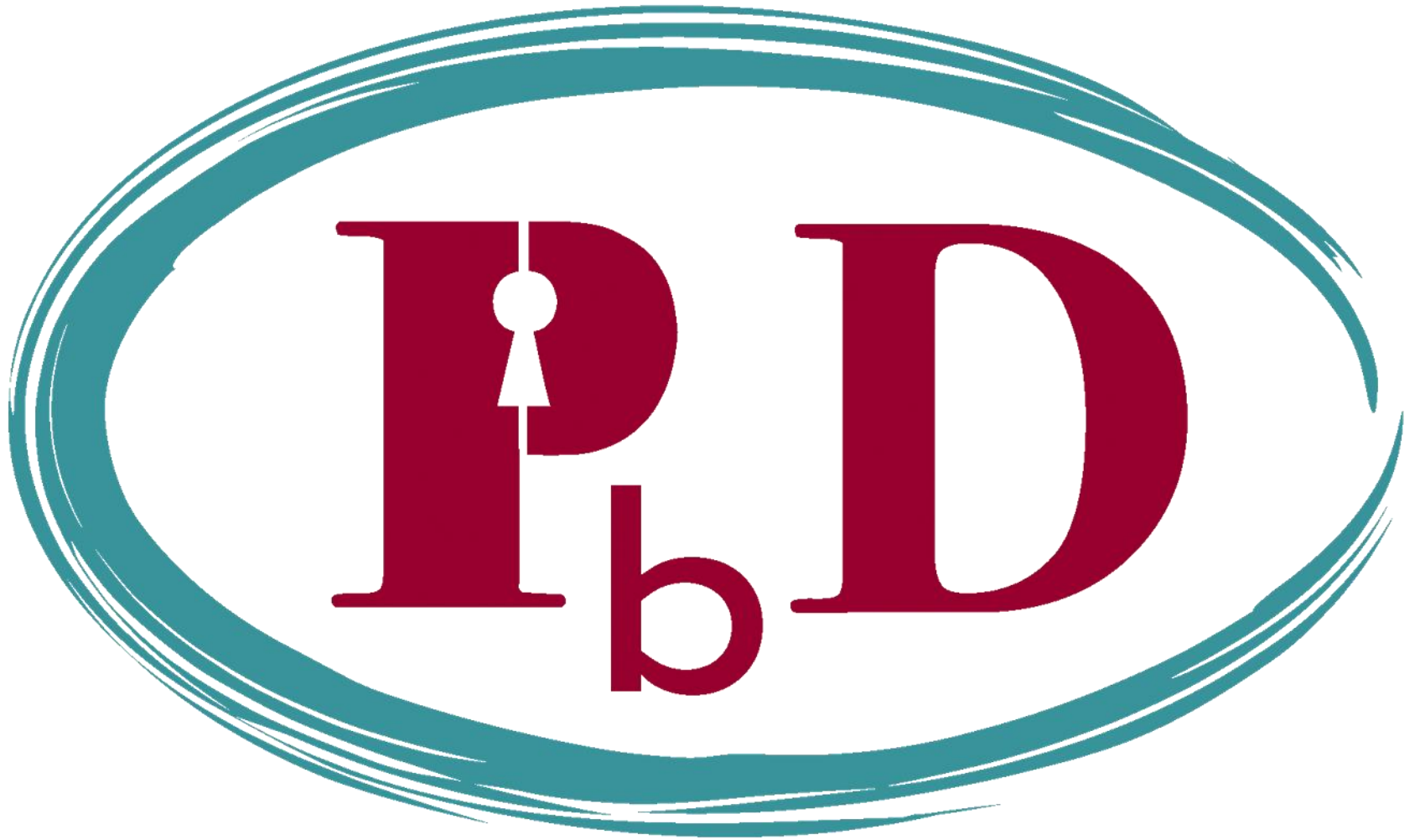
Robert Scheer

“For Democracy, Privacy is the Ball Game. Without the assurance of a zone of inviolate space, both physical and mental, that a citizen can inhabit without fear of observation by others, there is no guarantee of the essential sovereignty of the individual promised in the First and Fourth Amendments to the US Constitution. The totality of societal observation over the individual is the defining antithesis of freedom.”

How Data-Collecting Corporations and Snooping
Government Agencies Are Destroying Democracy
Robert Scheer

https://books.google.ca/books/about/They_Know_Everything_About_You.html?id=f5DCBAAAQBAJ&redir_esc=y

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>

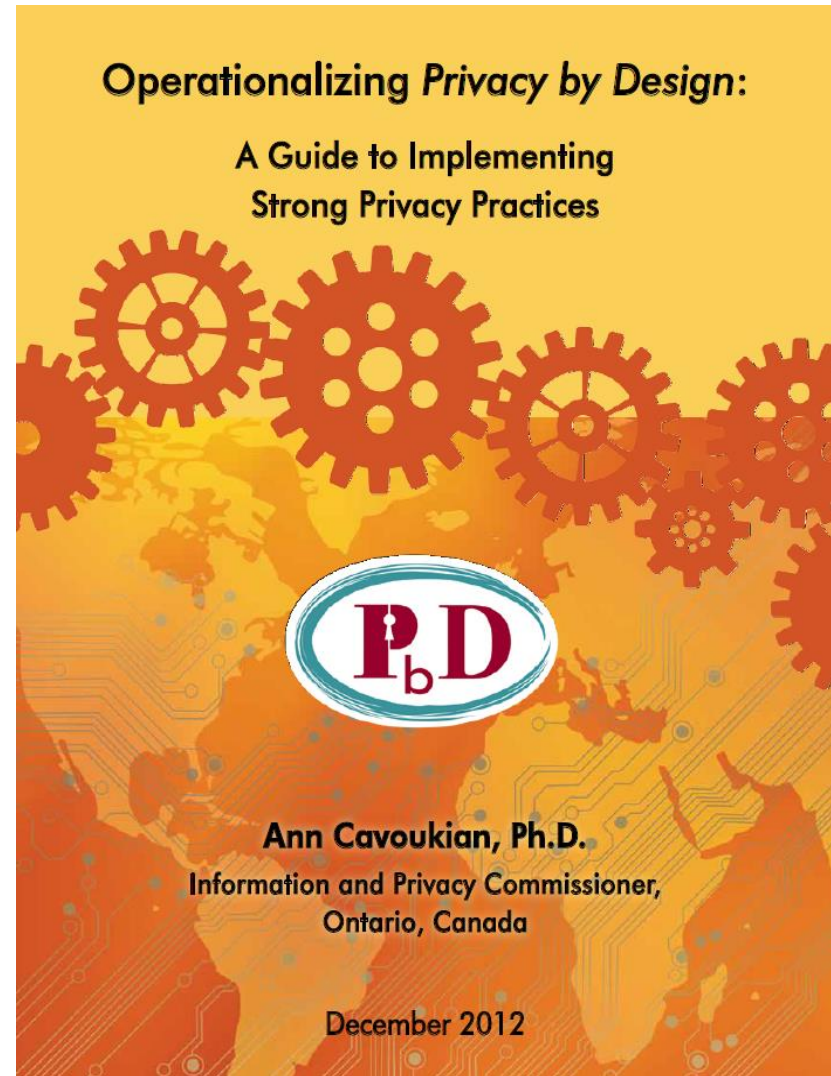
Operationalizing *Privacy by Design*

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

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 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

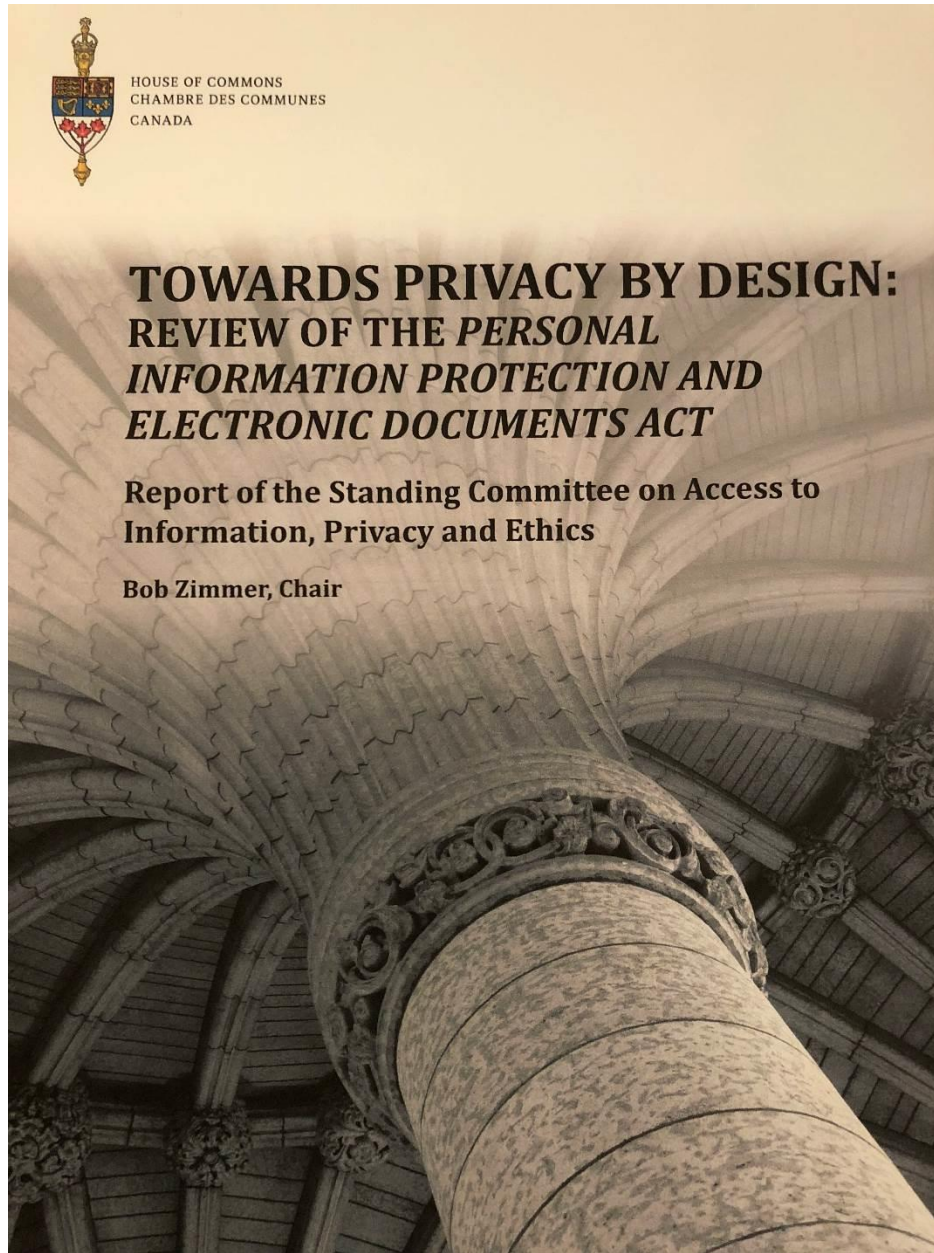


HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

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 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 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.

Privacy by Design as an ISO Standard

- Creation of 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.

Is the Tide Now Turning Towards Surveillance?

UK: Passing of The Investigatory Powers Bill

November, 2016

Petition to repeal new surveillance powers reaches 100,000 signatures

“Theresa May’s controversial **Investigatory Powers Bill** (AKA: Snooper’s Charter), which has been described as the most extreme snooping laws in a Western democracy, were approved by the House of Lords.”

The Telegraph
November 28, 2016

UK Mass Digital Surveillance Regime Ruled Unlawful

The Data Retention and Investigatory Powers Act, 2014 has been ruled to have breached E.U. law as it allows data to be harvested for reasons other than fighting serious crime.

The Guardian
January 30, 2018

<https://www.theguardian.com/uk-news/2018/jan/30/uk-mass-digital-surveillance-regime-ruled-unlawful-appeal-ruling-snoopers-charter>

Australia's "Assistance and Access" Bill

- Australia has legalized Backdoors to encrypted communications, allowing the government to break into encrypted emails intended to remain private.
- "Attempting to roll back the clock on security improvements which have massively benefited Australia and the entire global community is a disappointing development."

Setback in the Outback
Signal Blog
December 13th, 2018

<https://signal.org/blog/setback-in-the-outback/>

Is Surveillance Becoming the “New Normal” of the Internet?

**“Surveillance is the business
model of the Internet.”**

- Bruce Schneier

The Harvard Gazette
August 24, 2017

<https://news.harvard.edu/gazette/story/2017/08/when-it-comes-to-internet-privacy-be-very-afraid-analyst-suggests/>

RYERSON
UNIVERSITY

The Vital Need for Encryption!

Encryption is crucial to our privacy and freedom



ANN CAVOUKIAN

Encryption is crucial to our privacy and freedom

ANN CAVOUKIAN

Contributed to The Globe and Mail

Published Wednesday, Dec. 09, 2015 6:00AM EST

Last updated Wednesday, Dec. 09, 2015 6:00AM EST

THE GLOBE AND MAIL 

Comments

AA

Ann Cavoukian is executive director of the Privacy and Big Data Institute at Ryerson University and former information and privacy commissioner of Ontario

The aftermath of any major terrorist attack such as the recent tragedy in Paris appears to predictably include a call for new privacy-invasive policies that restrict freedom. After the attacks on 9/11, it was the passing of the USA PATRIOT Act; after the 2014 attack on Parliament Hill, it was the passing of Bill C-51. Throughout history, governments have always been a double-edged sword: We give them a monopoly on the use of force to protect us against the dystopian elements in our society, but in our constitutions, we have placed strong limits on the use of this force.

December 9, 2015

The Debate Over Encryption

Giving the government keys to encrypted software will make Americans less safe

By: Cindy Cohn

In response to the horrible terrorist attacks in Paris and San Bernardino, Calif., law enforcement and some ill-informed politicians are trotting out a demand that was soundly rejected more than 20 years ago: government “backdoors” or “keys” to encrypted data.

THE WALL STREET JOURNAL.

December 23, 2015

<http://www.wsj.com/articles/the-debate-over-encryption-the-backdoor-is-a-trapdoor-1450914316>

“Keys Under Doormats:

Mandating Insecurity by Requiring Government Access to All Data and Communications”

Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, Daniel J. Weitzner

Massachusetts Institute of Technology
Computer Science and AI Laboratory Technical Report
July 6, 2015

<https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf>

Finding a Needle in a Haystack

“Many would argue that granting intelligence agencies further powers to intercept, collect, decrypt and store exabytes of personal data only exacerbates their problem of finding the terrorist needle in the public haystack.”

The Economist,
January 19, 2015

What Works?

“The question asked repeatedly since the intelligence agencies embarked on their wholesale wiretapping of private citizens is, “does profiling hundreds of millions of good guys help to unmask the few dozen bad guys in their midst? . . . There is scant evidence that it does.”

The Economist,
January 19, 2015

**Targeted Surveillance
vs.
Indiscriminate Surveillance
(fishing expeditions)**

A Surveillance Winter: The Chilling Effect on Freedom

“Communications metadata, prized by Michael Hayden, were recently described by a task force set up to review the [Patriot Act] Section 215 metadata program as having *no use in stopping terror attacks* . . . many security experts insist that much more **targeted** surveillance works far better.”

Professor David Lyon,
Queen's University,
January 23, 2015

The Need for Both Privacy **And** Security (Straight from Homeland Security)

“You can’t have privacy without security ... To me, the most frustrating thing is when people treat privacy and security as if they were trade-offs.”

-Michael Chertoff,
2nd Secretary of Homeland Security
Huffington Post
October 3, 2015

NSA Chief Michael Rogers Stakes Out Pro-Encryption Position, in Contrast to the FBI

“Encryption is foundational to the future,” and arguing about it is a waste of time ... While there’s been a lot of talk about giving up some privacy for security ... both are paramount.”

The Intercept
Jan 21, 2016

<https://theintercept.com/2016/01/21/nsa-chief-stakes-out-pro-encryption-position-in-contrast-to-fbi/>

Tech group rejects call for data encryption 'backdoors'

"Weakening encryption ... in the name of national security simply does not make sense."

"Encryption is a security tool we rely on everyday to stop criminals from draining our bank accounts, to shield our cars and airplanes from being taken over by malicious hacks, ... **weakening encryption or creating backdoors ... for use by the good guys would actually create vulnerabilities to be exploited by the bad guys ... Weakening encryption is not a solution.**"

Information Technology Industry Council

November 20, 2015

<http://in.reuters.com/article/2015/11/19/tech-encryption-idINL1N13E2BV20151119>

Leading Crypto Expert strongly opposes creation of backdoors

“Rather than providing us with better security, the FBI’s efforts [to mandate the creation of crypto backdoors] **will torpedo it.**”

“**Encryption and other protections secure our systems ... and should never be undermined.**”

Susan Landau, PhD

Testimony for House Judiciary Committee Hearing on
“The Encryption Tightrope: Balancing Americans’ Security and Privacy”
March 1, 2016

“Misunderstanding Terrorism”: How the us vs. them Mentality Will Never Stop Attacks”

“Finding and stopping terrorists before they strike is often compared to looking for a needle in a haystack, a cliché that speaks to the difficulty of preventing a crime that, while deadly, is truly uncommon.”

“A new book, ‘Misunderstanding Terrorism’ by Dr. Marc Sageman, a veteran counterterrorism researcher and former CIA operations officer, argues that **this approach (sifting through the haystack in search of terrorists), even if carried to its fullest extension in a nightmare scenario for civil liberties, would still be ineffective, because jihadist terrorism is such a statistically rare phenomenon.**”

Murtaza Hussain
The Intercept
May 13, 2017

Government-fueled media hysteria over encryption begins

“It should come as no surprise that we turn to encryption to protect our interests ... No one wants to become the victim of fraud. No one wants their bank accounts emptied, or their personal information stolen.”

“Terrorism will not be defeated by outlawing encryption ... we must not fall into the trap of being distracted ... our right to privacy is crucial, and attempts to erode our privacy in the name of “national security” serve only to harm the innocent.”

neilalexander.eu
November 23, 2015

<http://neilalexander.eu/articles/2015/11/23/government-fueled-media-hysteria-over-encryption-begins>

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

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.

Breach Level Index,
2017

<http://breachlevelindex.com/>

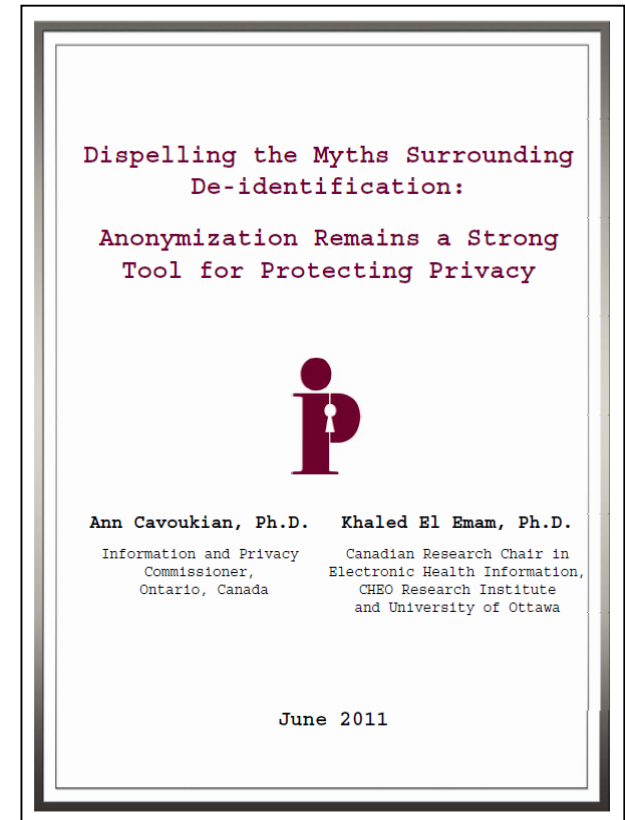
Data Minimization and De-Identification

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 Risk-Based 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

***SmartData:
Privacy by Design 2.0***

Context is Key

The Next Evolution in Data Protection: “SmartData”

Developed at by Dr. George Tomko at the Identity, Privacy and Security Institute, University of Toronto, *SmartData* represents privacy in the future with greater control of personal information.



Intelligent “smart agents” to be introduced into IT systems virtually – thereby creating “*SmartData*,” – a new approach to Artificial Intelligence, bottom-up, that will contextualize the field of AI .

SmartData: It's All About User Control

It's All About Context:

- Evolving virtual cognitive agents that can act as your proxy to protect your personally identifiable data;

Intelligent software agents will be evolved to:

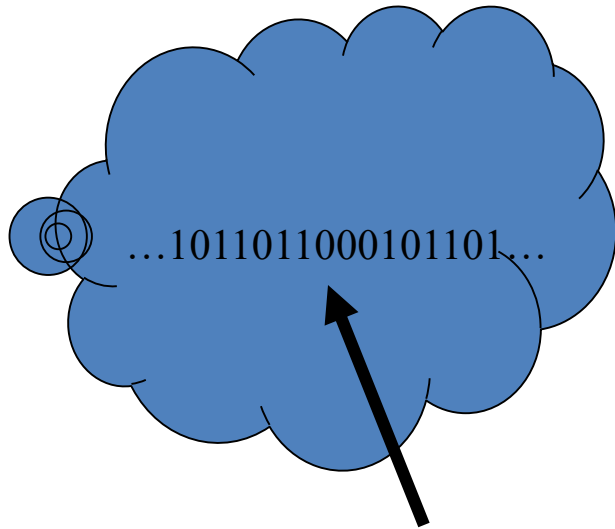
- Protect and secure your personal information;
- Disclose your information only when your personal criteria for release have been met;
- Put the *user* firmly in control –
Big Privacy, Radical Control!

Methods of Creating Intelligent SmartData Software Agents

- Top-down, rule-based design (traditional AI);
- Bottom-up “evolutionary robotics design;”
- The combination of a top-down and bottom-up (embodied cognition) hybrid will yield the most dynamic results.

Only SmartData will reside in the cloud: No Personal Information!

- Only a SmartData binary string will be transmitted



SmartData binary string – personal information is locked inside

- *There would never be any personal or proprietary “raw” data out in the open.*
- *The data would be securely housed “within” a SmartData agent.*

“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

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 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