# How Best to Embed Privacy and Security into Design? In Search of Much-Needed Research


## Ann Cavoukian, Ph.D.

**Executive Director**
**Privacy and Big Data Institute**
**Ryerson University**


**Invited Distinguished Seminar Series**
**Concordia University**
**June 15, 2017**

RYERSON UNIVERSITY

**“Civilization is the progress towards a society of privacy”**
**Ayn Rand**

Loss of privacy is the regression of a society towards an uncivilized society, devoid of freedom, innovation, and prosperity.

# 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.

# Let’s Dispel Some Myths

# Privacy ≠ 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!**

# *The Decade of Privacy by Design*


RYERSON UNIVERSITY

# *Adoption of "Privacy by Design" as an International Standard*

## Landmark Resolution Passed to Preserve the Future of Privacy

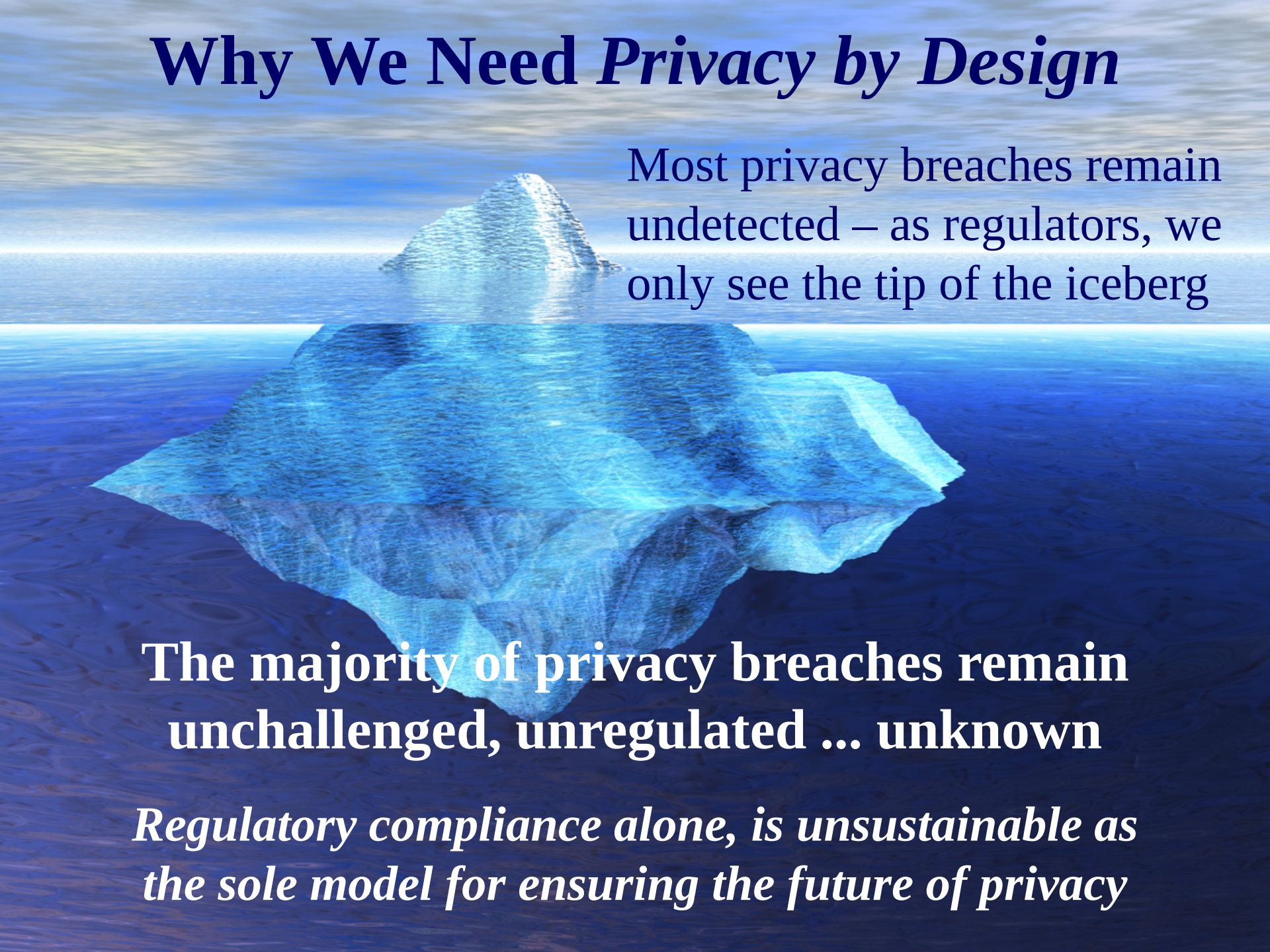
By Anna Ohlden – October 29th 2010 - http://www.science20.com/newswire/landmark_resolution_passed_preserve_future_privacy

**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 39 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. *Afrikaans (pending)*

RYERSON UNIVERSITY

# 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"***

RYERSON UNIVERSITY

# *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**.

PbD

www.privacybydesign.ca

Privacy by Design

*The 7 Foundational Principles*

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

*Privacy by Design* is a concept I developed back in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

*Privacy by Design* advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we realize that a more substantial approach is required — extending the use of PETs to PETS *Plus* — taking a positive-sum (full functionality) approach, not zero-sum. That's the "*Plus*" in PETS *Plus*: positive-sum, not the either/or of zero-sum (a false dichotomy).

*Privacy by Design* extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure.

Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy measures tends to be commensurate with the sensitivity of the data.

The objectives of *Privacy by Design* — ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following 7 Foundational Principles *(see over page)*:

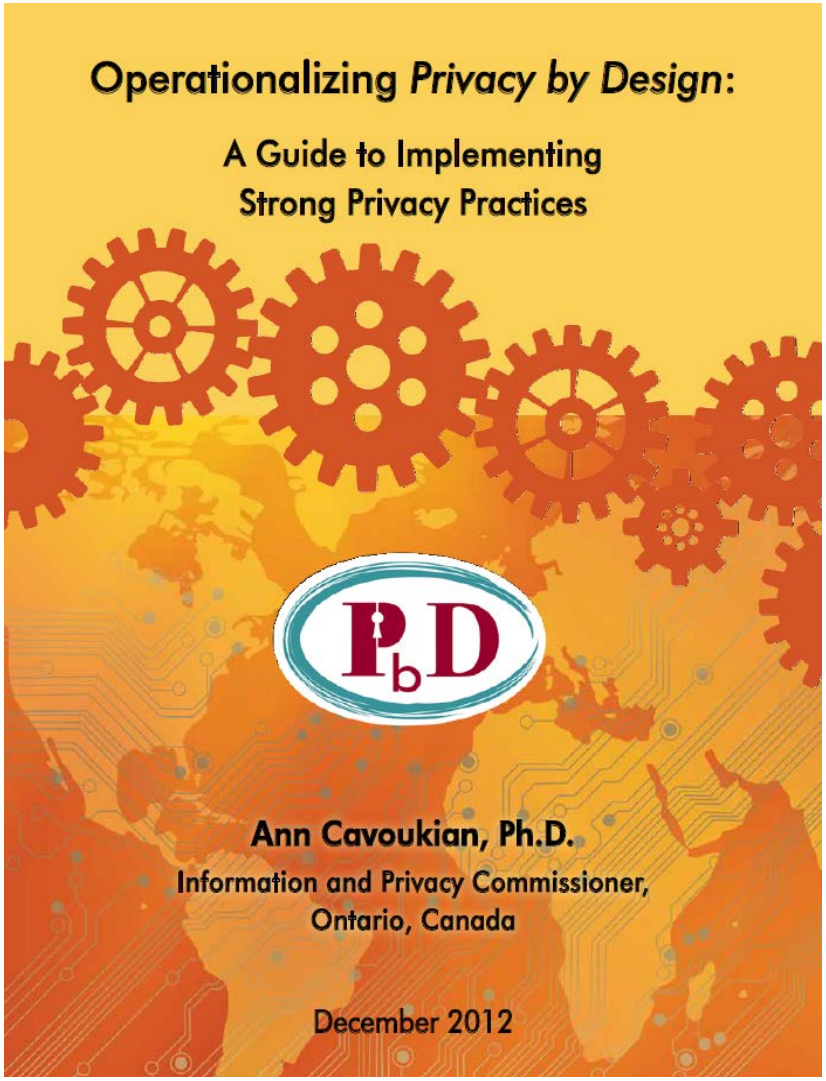
www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

RYERSON UNIVERSITY

# Operationalizing *Privacy by Design*

## *9 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;
- SmartData.



# *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

# EU-US Safe Harbor Framework Invalid: European Union Court of Justice

"The Court of Justice of the European Union (CJEU) has in its decision today declared that transfers of personal data from the EU to the US cannot rely on the Safe Harbor framework agreement."

Privacy Laws & Business
October 6, 2015
http://www.privacylaws.com/Int_enews_6_10_15

# Privacy Shield:
# More robust and sustainable solution needed

" I appreciate the efforts made to develop a solution to replace Safe Harbour but the Privacy Shield as it stands **is not robust enough** to withstand future **legal scrutiny** before the Court. **Significant improvements** are needed should the European Commission wish to adopt an adequacy decision, to respect the **essence** of key **data protection principles** with particular regard to necessity, proportionality and redress mechanisms. Moreover, it's time to develop a **longer term solution** in the transatlantic dialogue."

- Giovanni Buttarelli,
European Data Protection Supervisor

Press Release
Brussels,
May 30, 2016

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-11-PrivacyShield_EN.pdf

# 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 passed in the E.U. in 2016.
  - 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 markers, 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

RYERSON UNIVERSITY

# Is the Tide Now Turning Towards Surveillance?

# Obama Opens NSA's Vast Trove of Warrantless Data to Entire Intelligence Community

"WITH ONLY DAYS until Donald Trump takes office, the Obama administration … announced new rules that will let the NSA share vast amounts of private data gathered **without warrant, court orders or congressional authorization** with 16 other agencies, including the FBI, the Drug Enforcement Agency, and the Department of Homeland Security."

Alex Emmons
The Intercept
January 13, 2017

https://theintercept.com/2017/01/13/obama-opens-nsas-vast-trove-of-warrantless-data-to-entire-intelligence-community-just-in-time-for-trump/

# CBC Investigation Reveals Widespread use of IMSI Catchers by the RCMP

"After shrouding their own use of the technology in secrecy for years, the RCMP took the unprecedented step of speaking publicly about the devices — also known as Stingrays — to address public concern amidst mounting questions about their use."

- In response to the CBC's investigation, the RCMP publicly confirmed its use of cellphone surveillance devices in Canada.

CBC News
April 5, 2017

http://www.cbc.ca/news/technology/rcmp-surveillance-imsi-catcher-mdi-stingray-cellphone-1.4056750

# President Trump delivers final blow to Web browsing privacy rules

“President Donald Trump signed a repeal of online privacy rules that would have limited the ability of ISPs to share or sell customers' browsing history for advertising purposes.”

"President Trump has signed away the only rules that guarantee Americans a choice in whether or not their sensitive Internet information is sold or given away," said Chris Lewis, VP of consumer advocacy group Public Knowledge.

Jon Brodkin
Ars Technica
April 3, 2017

https://arstechnica.com/tech-policy/2017/04/trumps-signature-makes-it-official-isp-privacy-rules-are-dead/

# Congress's vote to Eviscerate Internet privacy could give the FBI massive power

"Many are outraged about congressional efforts to eviscerate Internet privacy regulations set by the Federal Communications Commission under President Barack Obama. But a frightening aspect to the bill remains underappreciated: If signed, it could result in the greatest legislative expansion of the FBI's surveillance power since 2001's Patriot Act."

Paul Ohm
Washington Post

http://wapo.st/2oeBKya?tid=ss_tw

# Congress's vote to eviscerate Internet Privacy (cont'd)

"What the new law would do is give ISPs the incentive and the congressional and presidential seal of approval to construct the richest database of Web surfing and app-usage behavior the world has ever seen. This will be a honeypot attracting the FBI and other law-enforcement agencies like flies."

Paul Ohm
Washington Post

http://wapo.st/2oeBKya?tid=ss_tw

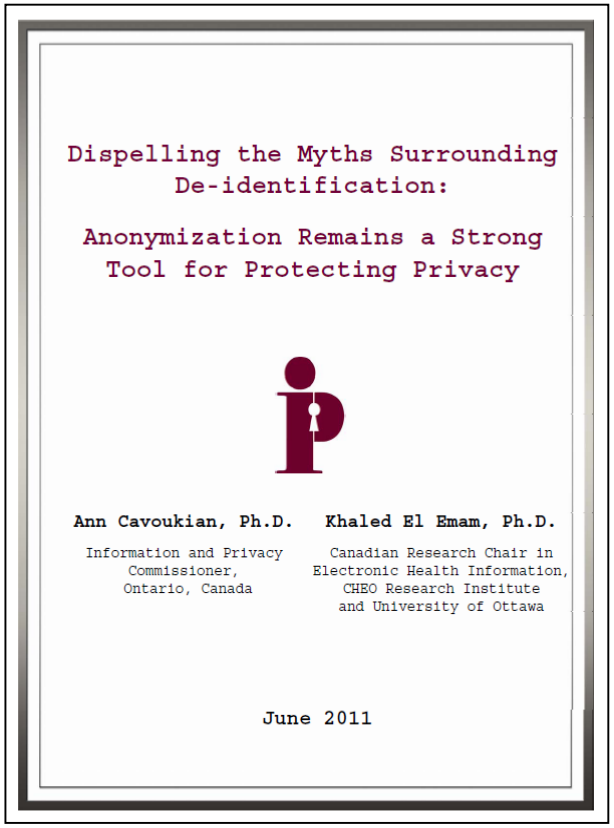
# *Data Minimization and De-Identification*

# 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.



Dispelling the Myths Surrounding De-identification:

Anonymization Remains a Strong Tool for Protecting Privacy

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

Khaled El Emam, Ph.D.
Canadian Research Chair in Electronic Health Information, CHEO Research Institute and University of Ottawa

June 2011

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

RYERSON UNIVERSITY

# Evidence that the Tool Works

- Dr. El Emam was approached to create a longitudinal public use dataset using his de-identification tool for the purposes of a global data mining competition – the Heritage Health Prize;
- Participants in the Heritage Health Prize competition were asked to predict, using de-identified claims data, the number of days patients would be hospitalized in a subsequent year;
- Before releasing the dataset created using Dr. El Emam's tool, the de-identified dataset was subjected to a strong re-identification attack by a highly skilled expert;
- The expert concluded the dataset could **not** be re-identified – Dr. El Emam's de-identification tool was highly successful!

# Evidence that Re-Identification is Extremely Difficult

- A literature search by Dr. El Emam et al. identified 14 published accounts of re-identification attacks on de-identified data;
- A review of these attacks revealed that one quarter of all records and roughly one-third of health records were re-identified;
- **However, Dr. El Emam found that only 2 out of the 14 attacks were made on records that had been properly de-identified using existing standards;**
- Further, only 1 of the 2 attacks had been made on health data, resulting in a **very low re-identification** rate of **0.013%.**

# 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.

# The Myth of Zero-Risk

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

1. Institute of Medicine:

2. HI Trust: Health Information Trust Alliance:

3. Council of Canadian Academies:

4. PhUSE Pharmaceutical Users Software Exchange:

5. NIST: De-Identification of Personal Information

# 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

# 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.

# Companies Should be Allowed to Innovate with De-Identified Data

"Re-Identification concerns are over-stated … anonymized data can, in many circumstances be used without fear of re-identification."

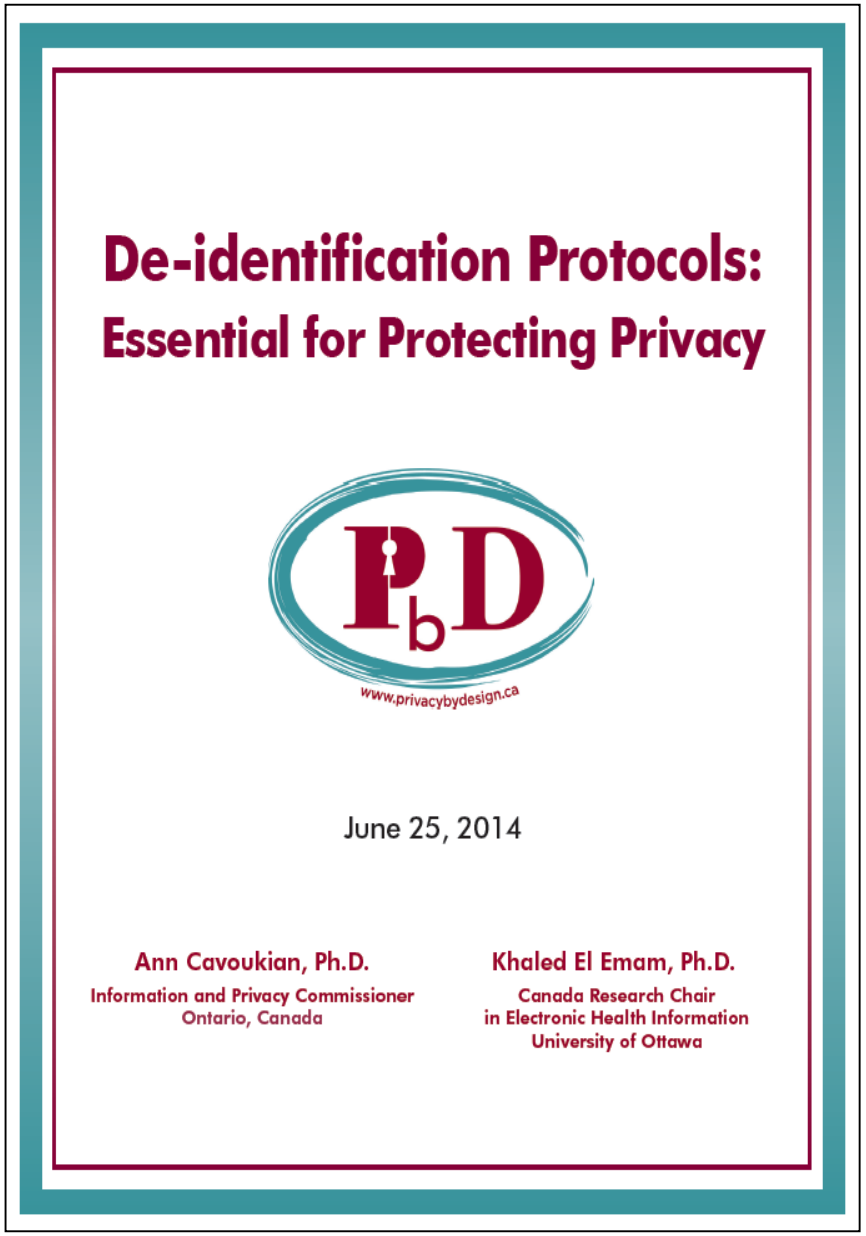
Information Technology and Innovation Foundation

January 17, 2014

RYERSON UNIVERSITY

*"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




RYERSON UNIVERSITY

# Internet of Things (IoT)

# Wireless and Wearable Devices

1) Wearable Computing:
   - Everyday objects
     - i.e. Google glass, Apple watch, Nymi band
2) Quantified Self:
   - Record information about one's habits, lifestyle and activities (Health, Fitness and sleep trackers)
3) Home Automation:
   - Computer controlled thermostats, light bulbs, smart meters, the smart grid, etc.

# The IoT of Wearables
# Mobile Health & Fitness Devices:
# Where's the Privacy?

"As mobile health and fitness apps and wearables gain popularity, privacy experts have raised concerns that companies are monetising personal medical information. There are thousands of health and fitness devices and apps on the market, but it is not always clear if users' data is kept confidential."

-Bridget Brennan,
The World Today,
April 28, 2015

RYERSON UNIVERSITY

# IoT Fears Relating to Tracking

"Earlier this year, Symantec Corp. analyzed a number of [wireless] wearable products and found that **all** hardware-based devices were **100% trackable**."

Anura Fernando
The Privacy Advisor
August 25, 2015

# Broadband Stakeholders Eye Security, Privacy of Internet of Things

"Some IoT devices are shipped with security flaws that can put end users at risk and negatively affect their internet experience, for a variety of reasons."

Broadband Internet Technical Advisory Group
Broadcasting & Cable
June 28, 2016

http://www.broadcastingcable.com/news/washington/broadband-stakeholders-eye-security-privacy-internet-things/157645

# Privacy and Security by Default

"With the personal data of millions potentially at stake, wearable manufacturers, whether their products are regulated as a medical device or not, **should incorporate as a default standards-based privacy and security controls into their product infrastructures."**

Anura Fernando
The Privacy Advisor
August 25, 2015

RYERSON UNIVERSITY

# FTC expresses concerns over Mobile Health Apps

- The U.S. Federal Trade Commission (FTC) has expressed concerns with the risks associated with the Health Information collected by the Apple Watch and HealthKit platform;
- Data stored in mobile health apps are not covered by HIPAA;
- **FTC found that 12 mobile health and fitness app developers were sharing user information with 76 different parties;**
- The FTC would like to ensure that developers have the necessary safeguards to protect personal health information.

# Remote Healthcare Monitoring and Wearable Devices: Privacy Risks

- **Third party monitoring removes control of one's information from the individual involved;**
- The nature of the devices may make it more difficult to obtain consent before data collection begins;
- Specific instances of data collection may not seem important on their own, but when aggregated, they can create a comprehensive picture of a person that may be extremely harmful to the individuals involved, especially in the hands of unauthorized third parties.

# What Apple has done to Protect Health Information

- Developers must have a privacy policy before they can access Apple's HealthKit;
- Users must give their consent before developers can access their Health Information;
- Data collected by the smartwatch is **encrypted** on the device;
- Apple will not allow any information collected through the HealthKit to be used for advertising or data-mining purposes;
- The Chair of the FTC praised Apple for taking steps critical to maintaining consumers' trust.

# A Much-Needed Privacy Standard for the Internet of Things

- Creating a common privacy standard now will earn user trust in privacy and security;
- 24 billion IoT devices before the decade is up;
- Whether this explosion amounts to the $1.7 trillion annual spend depends on the value this IoT delivers to users and trust in its privacy and security.

Jay Cline
Computerworld
December 1, 2015

http://www.computerworld.com/article/3010626/internet-of-things/a-privacy-standard-for-internet-of-things-suppliers.html

# EU Article 29 Working Party

- **Recommendations on the Internet of Things:**
  - **Make privacy the default setting … follow Privacy by Design;**
  - Delete all raw data after processing;
  - Respect a user's self-determination over their own data, and seek consent in a user-friendly way;
  - Be transparent about how a user's data is being used;
  - When sensors are continuously collecting one's personal data, remind users of this surveillance activity;
  - Ensure that data published to social platforms remain private, by default;
  - Users should not be penalized for failing to consent;
  - Data should be De-Identified, except when necessary.

# Privacy Commissioners Declaration on the Internet of Things

## 36th Int'l Conference of Data Protection and Privacy Commissioners

- The value of Internet of Things (IoT) is not only in the devices, but in the services that arise from their use;
- Connectivity is ubiquitous: it is the joint responsibility of all actors to ensure trust in connected systems : Transparency is Key;
- Protection should begin from the moment the data is collected:
  - **"Privacy by Design should be the key selling point of innovative technologies"**
- Strong, active and constructive debate is necessary to overcome the huge challenges presented by the developers of IoT.

September, 2014
Mauritius

RYERSON UNIVERSITY

# There is an Essential Need to Embed Privacy into IoT and Wearables, by Design

# For IoT To Succeed, Engineers Must Build in Privacy

"Most engineers are still wrapped up in the basic infrastructure of IoT. As a result, more abstract ideas such as personal privacy can quickly fall by the wayside."

Cliff Ortmeyer,
Global Solutions Development
April 24, 2015

# Consensual IoT

**“Consensual IoT means that IoT providers need to respect and take all measures in their power to protect user’s privacy and safety.”**

**“The term ‘consensual software’ means getting explicit consent from users to interact with them and to disclose their personal data.”**

Danielle Leong
May 23, 2017

https://dzone.com/articles/privacy-and-consensual-iot

# Great Need for Tech Solutions to Preserve Privacy!

# Machine Learning and AI

# When Algorithms Discriminate

" There is a widespread belief that software and algorithms that rely on data are objective. But software is not free of human influence. Algorithms are written and maintained by people, and machine learning algorithms adjust what they do based on people's behavior. As a result … algorithms can reinforce human prejudices."

Claire Cain Miller
The New York Times
July 9, 2016

http://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html

# Global Commission on Internet Governance

"Algorithms are not necessarily neutral: they incorporate built-in values and serve business models that can lead to unintended biases, discrimination or economic harm."

"The Increasing use of algorithms across society comes with considerable risks that the underlying data and algorithms could lead to unexpected false results, in particular when the algorithms are used for automated decision making."

Global Commission on Internet Governance

Ars Technica
June 22, 2016

http://arstechnica.com/tech-policy/2016/06/one-internet-global-internet-governance-report-analysis/

# The Tyranny of Algorithms

"The Tyranny of algorithms is nothing more than the tyranny of the past over the present." It's about how your past – reduced to bits of data, **often out of context** – dictates what happens to you today, and tomorrow. And that's why its important for us to continue to interrogate algorithms."

Torie Bosch
Future Tense
Slate.com
December 16, 2015

http://www.slate.com/blogs/future_tense/2015/12/16/the_tyranny_of_algorithms_a_future_tense_event_recap.html

RYERSON UNIVERSITY

# Call for Algorithmic Transparency

" When **algorithmic decision-making** can have life-altering consequences, it's critical to know what assumptions are baked into the code."

- There is a danger in taking algorithms without skepticism;
- There could be an unconscious bias;
- Transparency can provide an opportunity to verify results.

Torie Bosch
Future Tense
Slate.com
December 16, 2015

http://www.slate.com/blogs/future_tense/2015/12/16/the_tyranny_of_algorithms_a_future_tense_event_recap.html

# Statement on Algorithmic Transparency and Accountability
# Association for Computing Machinery

"The ubiquity of algorithms in our everyday lives is an important reason to focus on addressing challenges associated with the design and technical aspects of algorithms and preventing bias from the onset."

"There is … growing evidence that some algorithms and analytics can be opaque, making it impossible to determine when their outputs may be biased or erroneous."

ACM Public Policy Council
January 12, 2017

https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf

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

## *Context is Key*

RYERSON UNIVERSITY

# The Next Evolution in Data Protection:

# *"SmartData"*

**Developed 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 .**

RYERSON UNIVERSITY

# 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 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 Agents

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

# *An Innovative Approach:*

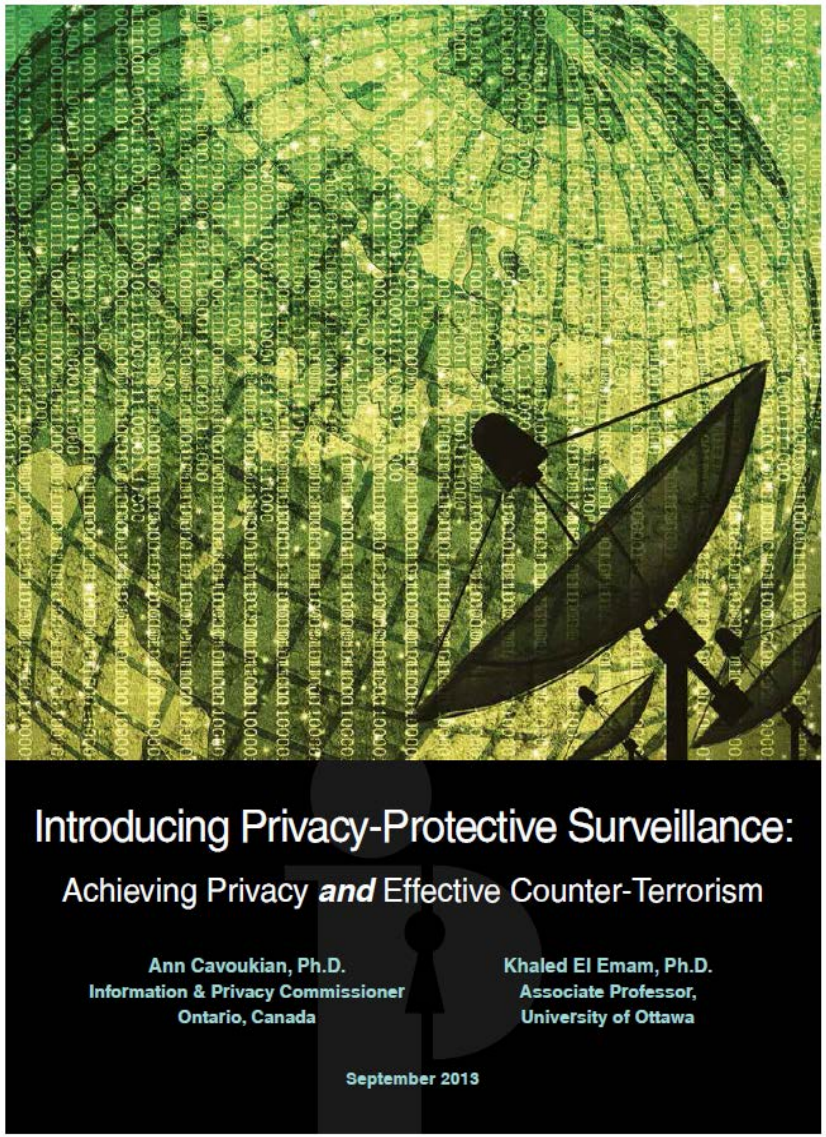
## *Applying Privacy by Design to Surveillance*

RYERSON UNIVERSITY

# Privacy-Protective Surveillance

*"As long as the threat of terrorism exists and the global conditions that instantiate those threats continue, effective measures will be needed to counteract terrorism.*

*At the same time, in order for a free and open society to function properly, privacy and civil liberties must be strongly protected."*




RYERSON UNIVERSITY

# Introducing PPS: Privacy-Protective Surveillance

- A new system of surveillance, which enables effective counter-terrorism measures to be pursued – **in a privacy-protective manner**;
- The underlying technology builds on Artificial Intelligence, advances in cryptography involving **Homomorphic Encryption**, and **Probabilistic Graphical Models** (involving Bayesian Networks).

# Summary of PPS

Privacy Protective Surveillance is a positive-sum, “win-win” alternative to current counter-terrorism surveillance systems. It incorporates two primary objectives in its design:

1. An AI system consisting of feature detection that scans the Web and related databases using a **“blind-sight” procedure** to detect digital evidence relating to potentially suspicious terrorist activity by some, without infringing on the privacy of unrelated individuals;
2. A technological infrastructure to ensure that any personally identifying information (“PII”) on unsuspected individuals is not collected and, in those associated with targeted activity, encrypted PII will only be divulged with judicial authorization (a warrant issued by the court).

# "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

http://privacyelephant.blogspot.ca/2016/11/privacy-by-design-ready-for-takeoff.html

# 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:

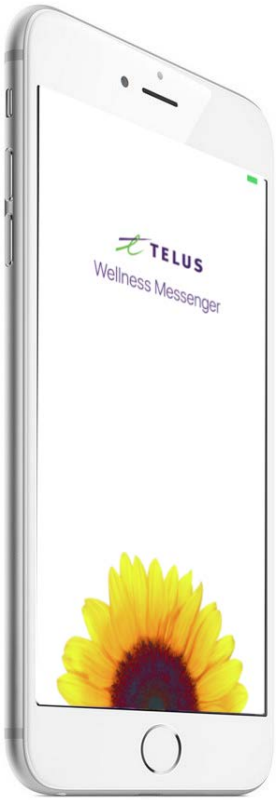
- Darren Entwhistle, CEO of TELUS Inc.
- Michael Chertoff, 2nd Secretary of U.S. Homeland Security
- Gilles de Kerchove, Director of E.U. Counter Terrorism
- Greg Wolfond, CEO of SecureKey

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




TELUS

# Wellness Messenger

## Privacy and Security by Design

**June 2017**

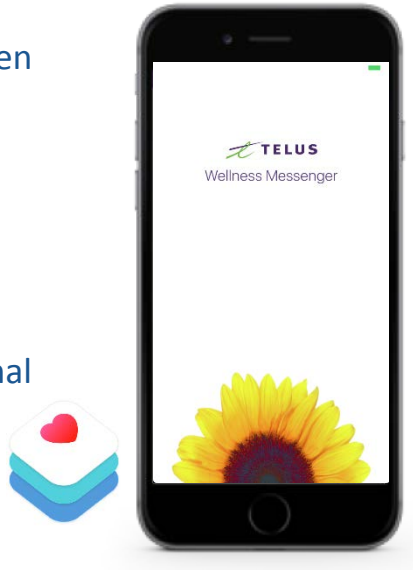
CERTIFIED PbD RYERSON UNIVERSITY

RYERSON UNIVERSITY

# TELUS Wellness Messenger (TWM)

A user-centric mobile solution that allows for the secure sharing of your wellness data in a user-managed, person-to-person, messaging ecosystem with a user-defined circle of trust: you're in control;

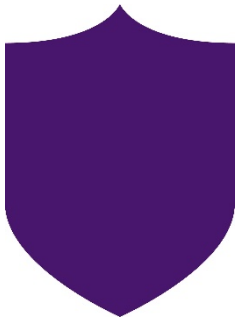
- Provides secure access to user's on-device Apple HealthKit data that has been collected and stored by various Wellness & Fitness Applications & Devices;
- Allows on-device Apple HealthKit data to be shared securely;
- Enables secure sending, receiving and person-to-person request for wellness data;
- Biometric authentication-based user-controlled data sharing enabled with additional layers of OS and application security;
- Provides users with a way to securely track wellness across wearable ecosystems;
- **Data privacy and authorization is managed and controlled completely by the user: privacy is the default setting**.




RYERSON UNIVERSITY

# Pillars of Privacy and Security Embedded in Design

**Privacy and Security top of mind for both Design and Development of TWM Application**



**Authentication**
**Access Restrictions**
**Data Encryption and Secure Storage**

**User Transparency & Control**
**Explicit User Consent**
**Data Containment**

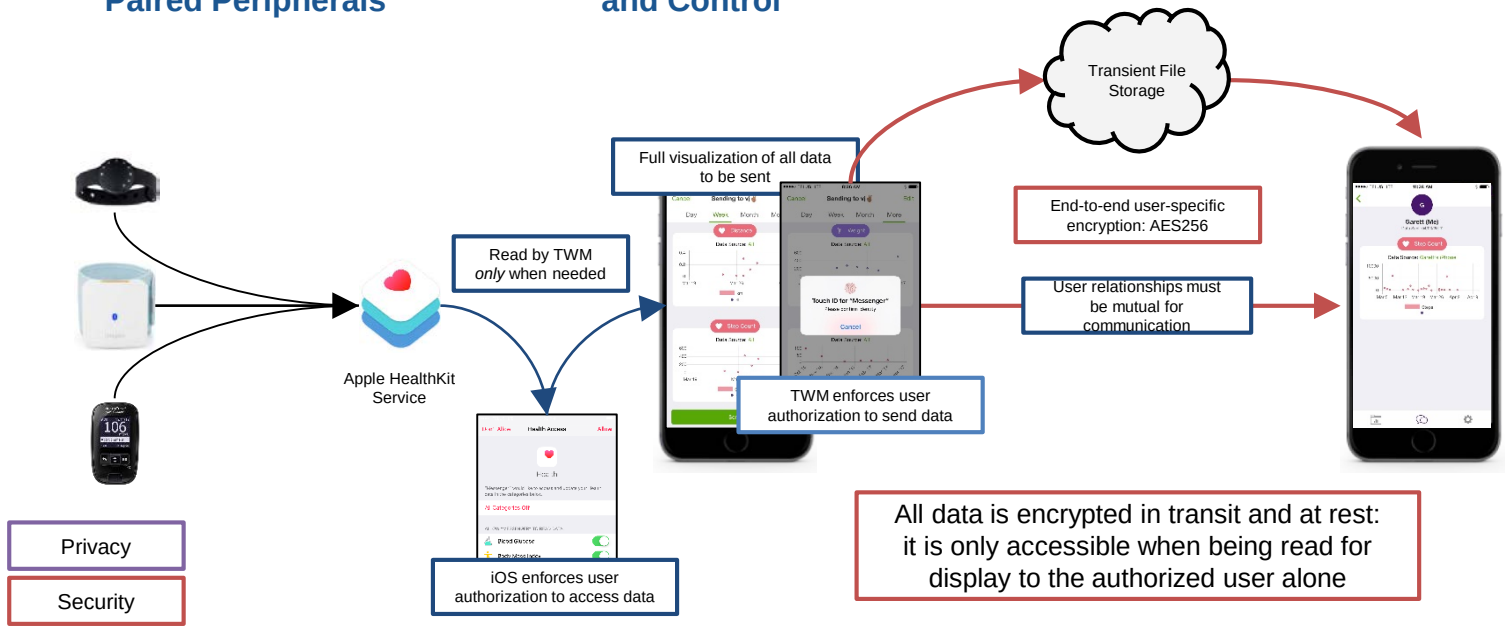
# Privacy and Security as the Default

## Wellness Data Read from Paired Peripherals

## User Authorization and Control

## File and Message Transfer

## Data Retention




**7** day server lifetime

**14** day device lifetime

TWM also purges all shared data if the relationship ends

RYERSON UNIVERSITY

# 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;
- 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.

**Executive Director**
**Privacy and Big Data Institute**
**Ryerson University**

**285 Victoria Street**
**Toronto, Ontario**
**M5B 2K3**

**Phone: (416) 979-5000 ext. 3138**

**ann.cavoukian@ryerson.ca**



ann.cavoukian@ryerson.ca

twitter.com/AnnCavoukian


RYERSON UNIVERSITY