

The Need to Proactively Embed Privacy, by Design into Your Operations

Ann Cavoukian, Ph.D.

Executive Director

**Global Privacy & Security by Design Centre
Toronto, Canada**

**Future of Privacy Forum Webinar
June 18th, 2019**

Let's Dispel The Myths

Privacy \neq Secrecy

Privacy is *not* about having
something to hide

Privacy = Control

Privacy = Personal Control

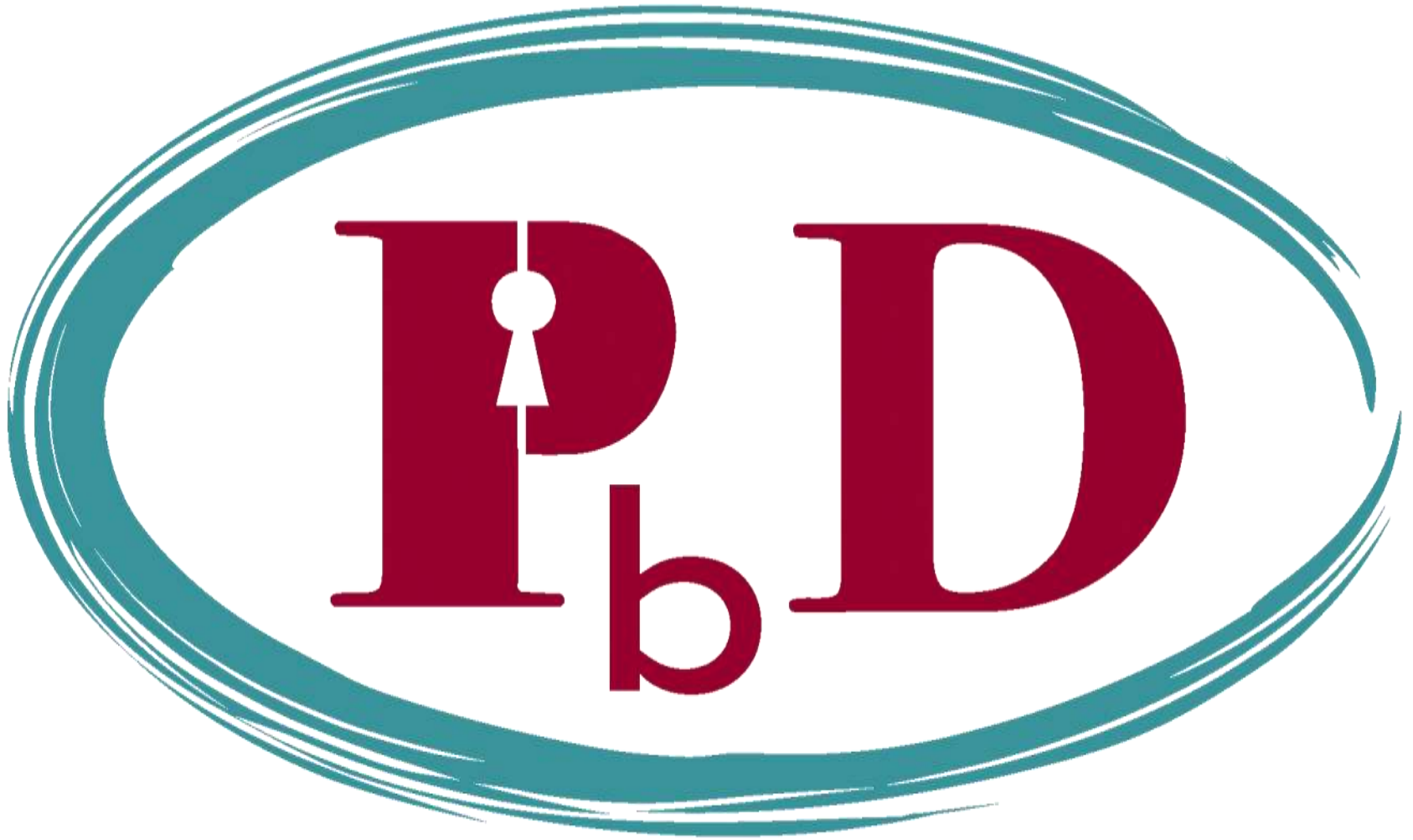
- **User control is critical**
- **Freedom of choice**
- **Informational self-determination**

Context is key!

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

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

The Decade of Privacy by Design



Adoption of “Privacy by Design” as an International Standard

Landmark Resolution Passed to Preserve the Future of Privacy

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

JERUSALEM, October 29, 2010 – A landmark Resolution by Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, was approved by international Data Protection and Privacy Commissioners in Jerusalem today at their annual conference. The resolution recognizes Commissioner Cavoukian's concept of Privacy by Design - which ensures that privacy is embedded into new technologies and business practices, right from the outset - as an essential component of fundamental privacy protection.

Full Article:

http://www.science20.com/newswire/landmark_resolution_passed_preserve_future_privacy

Why We Need *Privacy by Design*

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

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

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

Privacy by Design: Proactive in 40 Languages!

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

Two Essentials to Privacy by Design

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

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

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

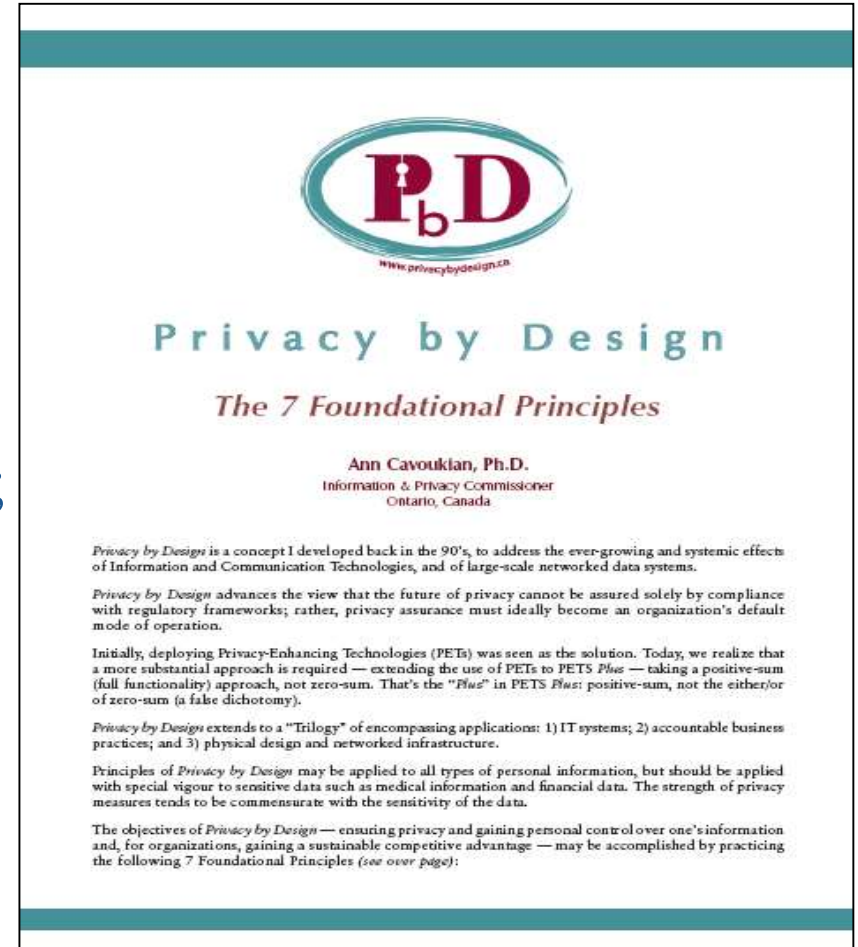
*Change the paradigm
from a zero-sum to
a “positive-sum” model:
Create a win-win scenario,
not an either/or (vs.)
involving unnecessary trade-offs
and false dichotomies ...*

replace “vs.” with “and”

Privacy by Design:

The 7 Foundational Principles

1. *Proactive* not *Reactive*:
Preventative, not Remedial;
2. Privacy as the *Default* setting;
3. Privacy *Embedded* into Design;
4. *Full* Functionality:
Positive-Sum, not Zero-Sum;
5. End-to-End **Security**:
Full Lifecycle Protection;
6. Visibility **and** Transparency:
Keep it **Open**;
7. Respect for User Privacy:
Keep it **User-Centric**.



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

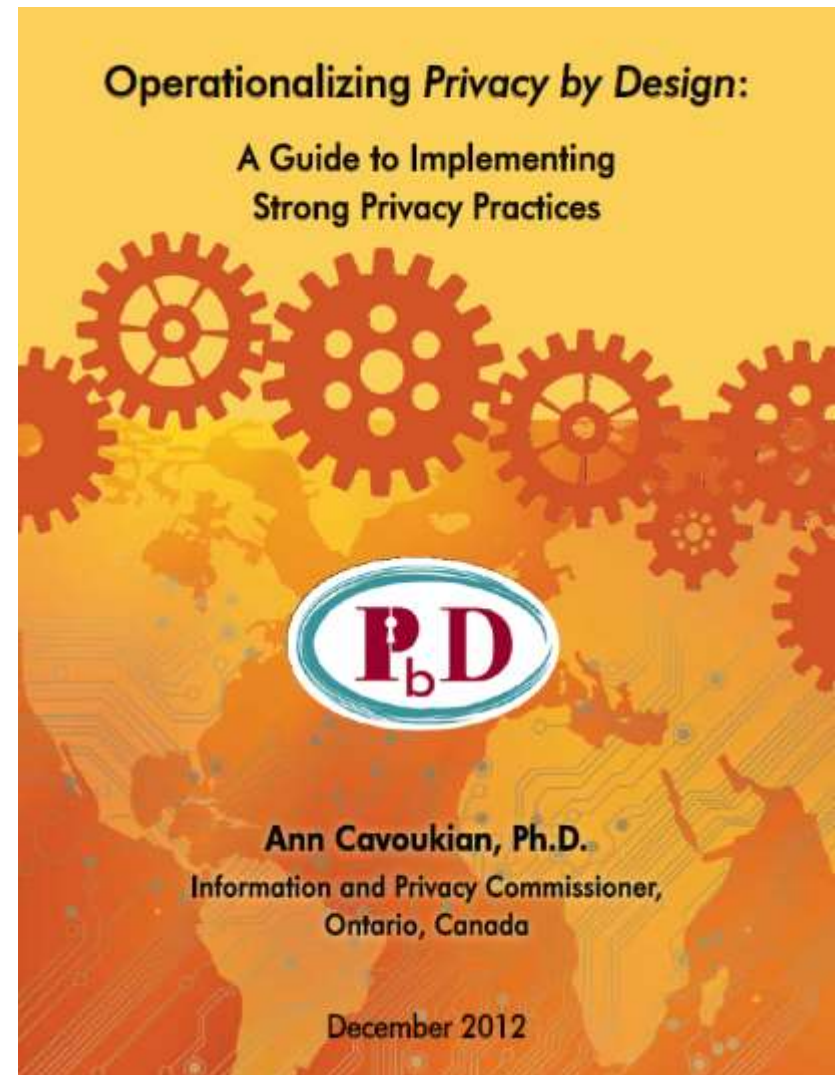
Operationalizing *Privacy by Design*

11 PbD Application Areas

- CCTV/Surveillance cameras in mass transit systems;
- Biometrics used in casinos and gaming facilities;
- Smart Meters and the Smart Grid;
- Mobile Communications;
- Near Field Communications;
- RFIDs and sensor technologies;
- Redesigning IP Geolocation;
- Remote Home Health Care;
- Big Data and Data Analytics;
- Privacy Protective Surveillance;
- SmartData.

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

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



Letter from JIPDEC – May 28, 2014

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

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

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

Cost of Taking the Reactive Approach to Privacy Breaches

Proactive



**Class-Action
Lawsuits**

**Damage to
One's Brand**

Reactive



**Loss of Consumer Confidence
and Trust**

GDPR

General Data Protection Regulation

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

E.U. General Data Protection Regulation

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

The Similarities Between PbD and the GDPR

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

Privacy Commissioner of Canada: Annual Report

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



HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

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

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

Bob Zimmer, Chair

42nd Parliament, First Session
February, 2018

Privacy by Design Certification

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

www.ryerson.ca/pbdce/certification

Privacy: 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*

First “Privacy Marketplace”

International Consumer Electronics Show, Las Vegas



*Victor Cocchia
CEO, Vysk
Speaking at CES: Jan, 2015*

“ 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.”

Consumers Value Privacy



“ 75 per cent will not buy a product from a company — no matter how great the products are — if they don’t trust the company to protect their data ”

Source: 2018 IBM, Harris Poll

Privacy Accelerates Sales & Investments

“ Evaluating a company’s privacy practices is now part of this firm’s due diligence, especially when companies are storing customer data in cloud services. ”



Steve Herrod of the VC firm, General Catalyst, told *The Privacy Advisor* that

The Business Case for Privacy



1. Accelerate Sales Cycles
2. Grow Customer Loyalty and Trust
3. Reduce Privacy Compliance Costs
4. Mitigate Penalties
5. Future-proof Your Defensibility and reduce Litigations and Enforcements with Strong Proof of Records

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;

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.

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/>

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

Consumer Confidence *(Cont'd)*

- 62 % of respondents say they would “not at all be likely” to repeat a purchase from a company that had shared their personal information with a data broker;
- A growing awareness about companies’ uses of consumer data will lead consumers to expect simpler, much more graphical privacy policies – *“misuse and abuse of data will impact profitability;”*
- **Companies should respond by “stress-testing” their data operations, and turn their privacy policies into a marketing opportunity.**

— 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!

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>

Petition to repeal new surveillance powers reaches 100,000 signatures (cont'd)

“They require internet providers to store customers’ web histories for 12 months and make those records available to police, and write computer hacking by spy agencies into law.”

“The petition warns that “With this bill, they will be able to hack, read and store any information from any citizen's computer or phone, without even the requirement of proof that the citizen is up to no good.”

The Telegraph
November 28, 2016

**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-scared-analyst-suggests/>

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

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 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>

Decentralization

“Broken by Design”

**“How the Internet has turned into
a tool that subverts freedom”**

Mike Mason
Aion Network
November 21st, 2019

**If You Value Freedom ...
Then You Value Privacy**

The Curse of Centralization

Massive centralization of personal data leads to unauthorized tracking and surveillance, turning the Internet into an opposing force – one that leads us away from freedom.

Tim Berners-Lee, the creator of the WWW. said: “I was devastated”

- The centralized model of data collection on the Web has led to massive tracking and surveillance, which has devastated its creator, Tim Berners-Lee;**
- He indicated that we must now stop centralization and turn to de-centralized models.**

Katrina
Brooker,
Vanity Fair,
July 1st, 2018

Decentralization of Data: The Way Forward

- Return control of one's data back to the data subject, where it belongs;
- decentralized data, belonging to the individual, may be securely stored in secure enclaves in the cloud.

Blockchain: A Public Records Repository

Blockchain technology is described as a **decentralized public ledger** for the recording of all online transactions that have ever been executed:

- The 'chain' continuously grows as 'completed' blocks are added to it, with a new set of recordings;
- The blocks are added in a linear, chronological order, creating a permanent, public record of all transactions;
- This public ledger facilitates and validates all public transactions;
- It enforces and moderates access-control based on digital signatures – (programmable permissions);
- It stores tamper-proof logs of correct (audited) executions.

“Privacy by Design – Ready for Takeoff”

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

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

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

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

Founding Members include:

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

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

International Council on Global Privacy and Security, by Design

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

www.gpsbydesign.org

Privacy by Design: The Global Privacy Framework

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



<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.
Executive Director
Global Privacy & Security by Design Centre

Phone: (416) 357-2818

ann.cavoukian@gpsbydesigncentre.com



ann.cavoukian@gpsbydesigncentre.com



twitter.com/AnnCavoukian