The Vital Need for Privacy and Security by Design

Ann Cavoukian, Ph.D.

Executive Director

Global Privacy & Security by Design Centre

Technion Summer School on Cyber Security

Haifa, Israel

September 9, 2020

Let’s Dispel The Myths

Privacy ≠ Secrecy

Privacy is *not* about having something to hide

Privacy = Control

Privacy = Personal Control

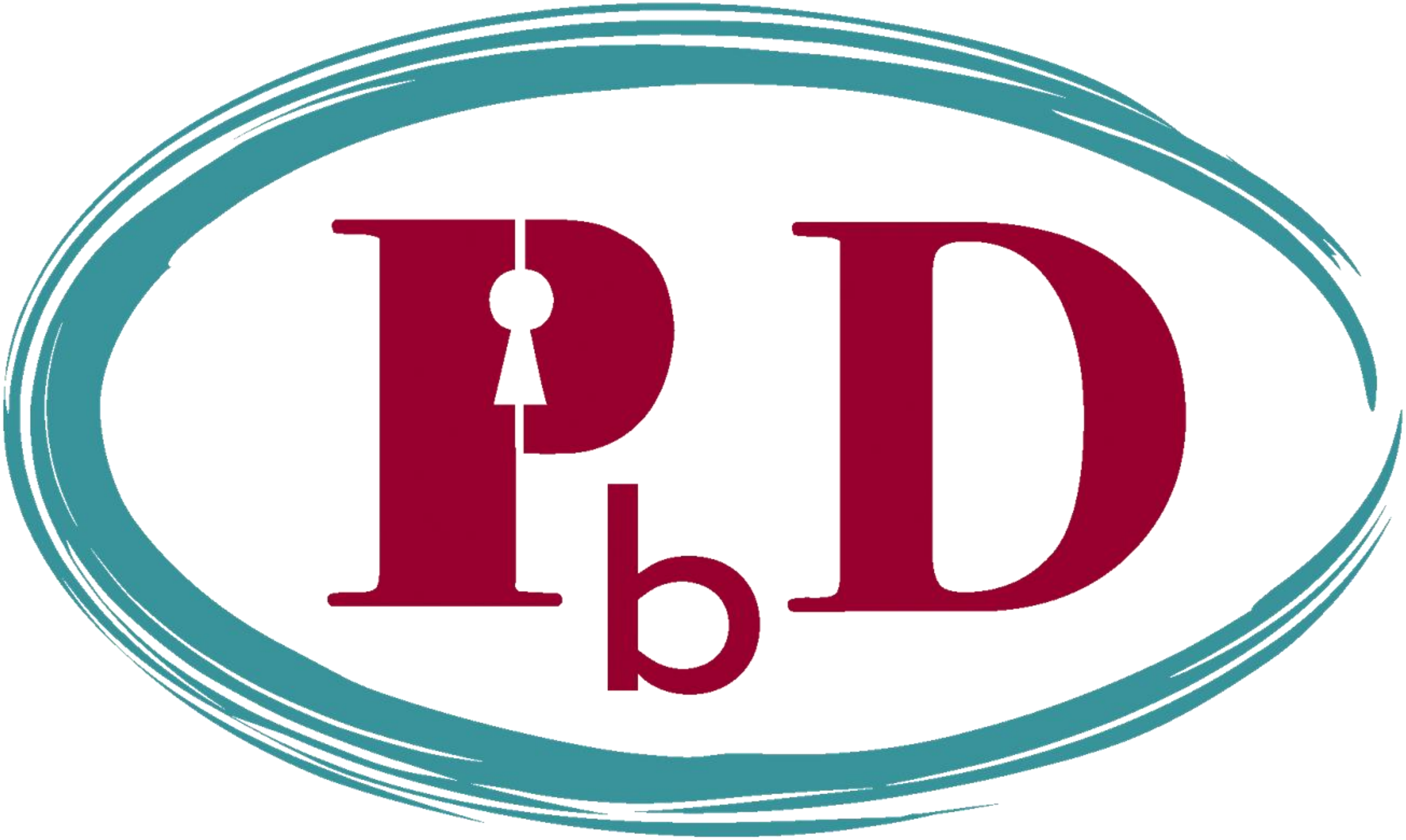
- User control is critical
- Freedom of choice
- Informational self-determination

Context is key!

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

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

The Decade of Privacy by Design



Adoption of "Privacy by Design" as an International Standard

Landmark Resolution Passed to Preserve the Future of Privacy

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

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

Full Article:

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

Why We Need *Privacy by Design*

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

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

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

Privacy by Design: Proactive in 40 Languages!

1. English

2. French

3. German

4. Spanish

5. Italian

6. Czech

7. Dutch

8. Estonian

9. Hebrew

10.Hindi

11.Chinese

12.Japanese

13.Arabic

14.Armenian

15.Ukrainian

16.Korean

17.Russian

18.Romanian

19.Portuguese

20.Maltese

21.Greek

22.Macedonian

23.Bulgarian

24. Croatian

25.Polish

26.Turkish

27.Malaysian

28.Indonesian

29.Danish

30.Hungarian

31.Norwegian

32.Serbian

33.Lithuanian

34.Farsi

35.Finnish

36.Albanian

37.Catalan

38. Georgian

39. Urdu

40. Tamil

41. Afrikaans (pending)

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**.

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)*:

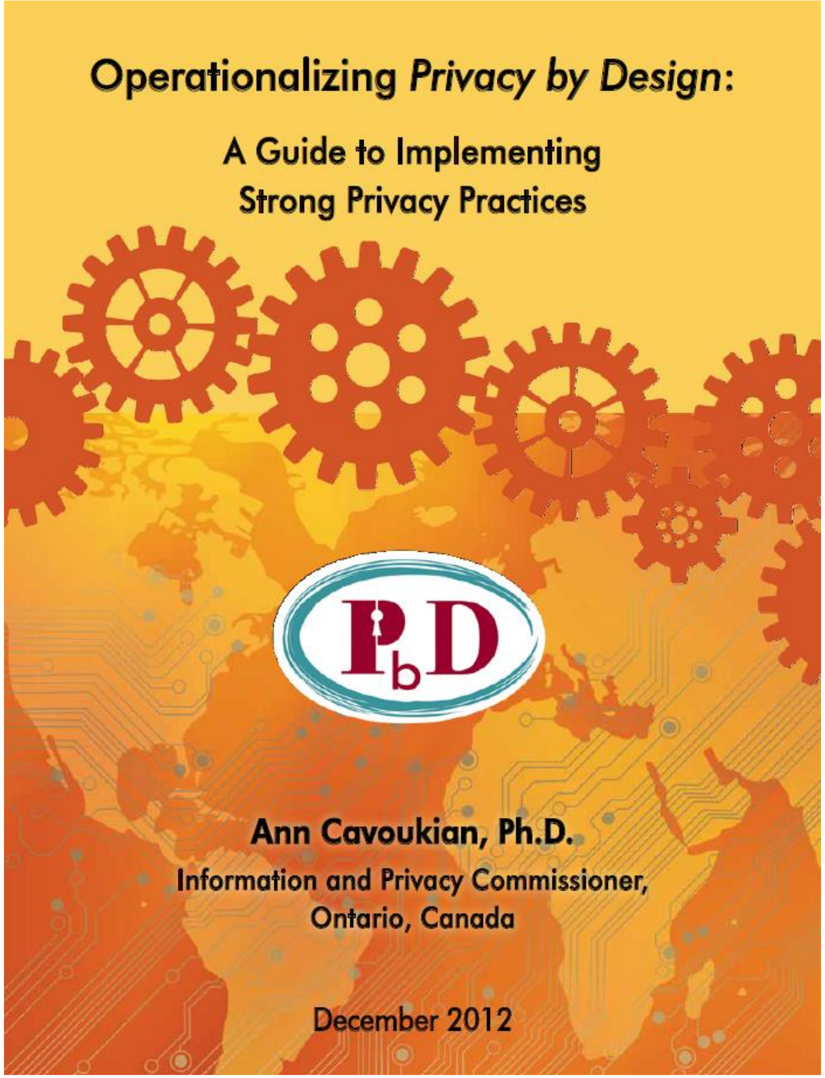
http://www.ryerson.ca/pbdce/papers/
http://www.ontla.on.ca/library/repository/mon/24005/301946.pdf

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



Operationalizing *Privacy by Design*:

A Guide to Implementing
Strong Privacy Practices

PbD

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

December 2012

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 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

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

http://www.telegraph.co.uk/technology/2016/11/28/petition-repeal-uks-new-surveillance-powers-reaches-100000-signatures/

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 then 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

http://www.telegraph.co.uk/technology/2016/11/28/petition-repeal-uks-new-surveillance-powers-reaches-100000-signatures/

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/

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

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2918779

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

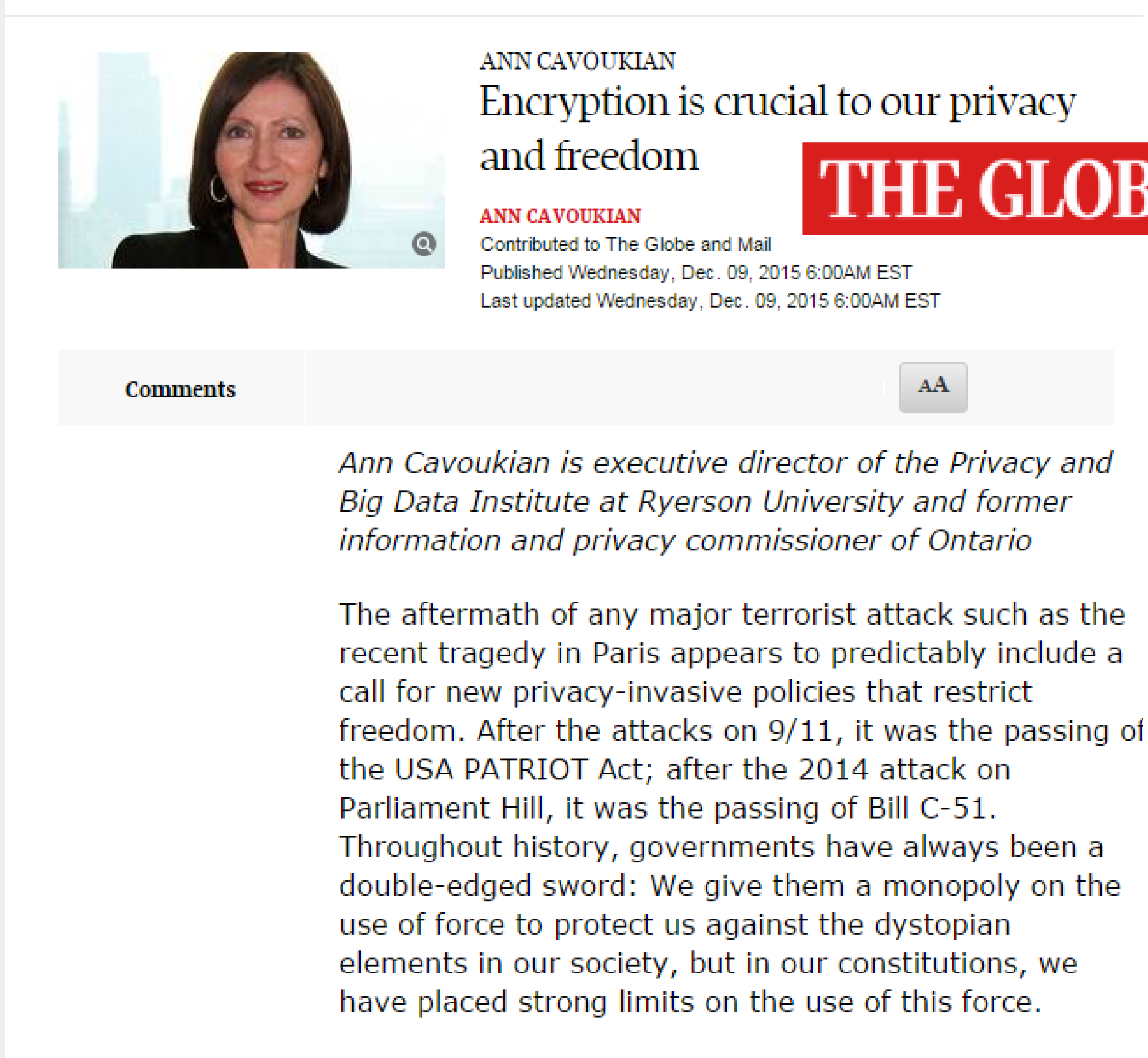
http://www.hldataprotection.com/2017/05/articles/news-events/upcoming-webinar-on-cybersecurity-and-the-internet-of-things/?utm_source=dlvr.it&utm_medium=twitter

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

THE GLOBE AND MAIL

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

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

https://theintercept.com/2017/05/13/misunderstanding-terrorism-how-the-us-vs-them-mentality-will-never-stop-attacks/

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

Facial Recognition

Facial Recognition Technology

- Facial recognition technology is largely invisible: you don’t know it’s operating in the background;
- Your facial image is the most sensitive biometric, deserving the strongest protection possible.

Facial Recognition Applications

- Invisibly, coming to a mall near you!
- Cadillac Fairview Mall – Alberta, Canada, a major fiasco: Facial images were being captured invisibly, with

No Notice,

No Consent,

No Control!

An Amazing Israeli company, D-ID, Protects Identities from Face Recognition Technologies

- Faces have become our digital identifiers. They must be strongly protected because unlike passwords, you cannot change your face.
- As more systems adopt facial recognition, the risk to privacy escalates dramatically. All organizations that handles images – corporations, governments, and security agencies – face new challenges involving regulatory requirements, growing privacy concerns and sensitive security issues.

D-ID: Protecting Identities from Face Recognition Technologies

- D-ID’s groundbreaking technology produces images that are unrecognizable to face recognition algorithms, while keeping them similar to the human eye;
- D-ID’s facial distortion is specifically designed to make it difficult for AI to overcome.

CoVid 19 and the Push for Contact Tracing

Digital Contact Tracing Will Fail Unless Privacy is Respected, Experts Warn

- 300 Experts/Epidemiologists from 26 countries globally have signed a joint letter warning that unless governments build contact- tracing technology in a privacy-protective manner, it will fail;
- “Such apps can otherwise be repurposed to enable unwarranted discrimination and surveillance … It is vital we do not create a tool that enables large-scale data collection on the population, now or at a later time.”

The Guardian

Second Open Letter from Experts Fearing that Contact-Tracing Could be Used to Surveil People

- 177 cybersecurity experts warn that the British government's contact-tracing App could be used to surveil people, even after the coronavirus has ended.

The Apple-Google API

- The Apple-Google Exposure Notification API is totally privacy-protective, leaving no identifiable personal data, nor geolocation data: Using Bluetooth beacons that change every 15 minutes (which are also encrypted using AES), if one chooses to use the App built upon this framework, you would be notified if you had been exposed to someone who had self-reported as being CoVid 19-positive.
- No personal data is recorded whatsover!

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 <u>and</u> Security; Privacy <u>and</u> 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