Embed Privacy in your IT Solutions: Privacy by Design

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario

Banking on Israeli IT

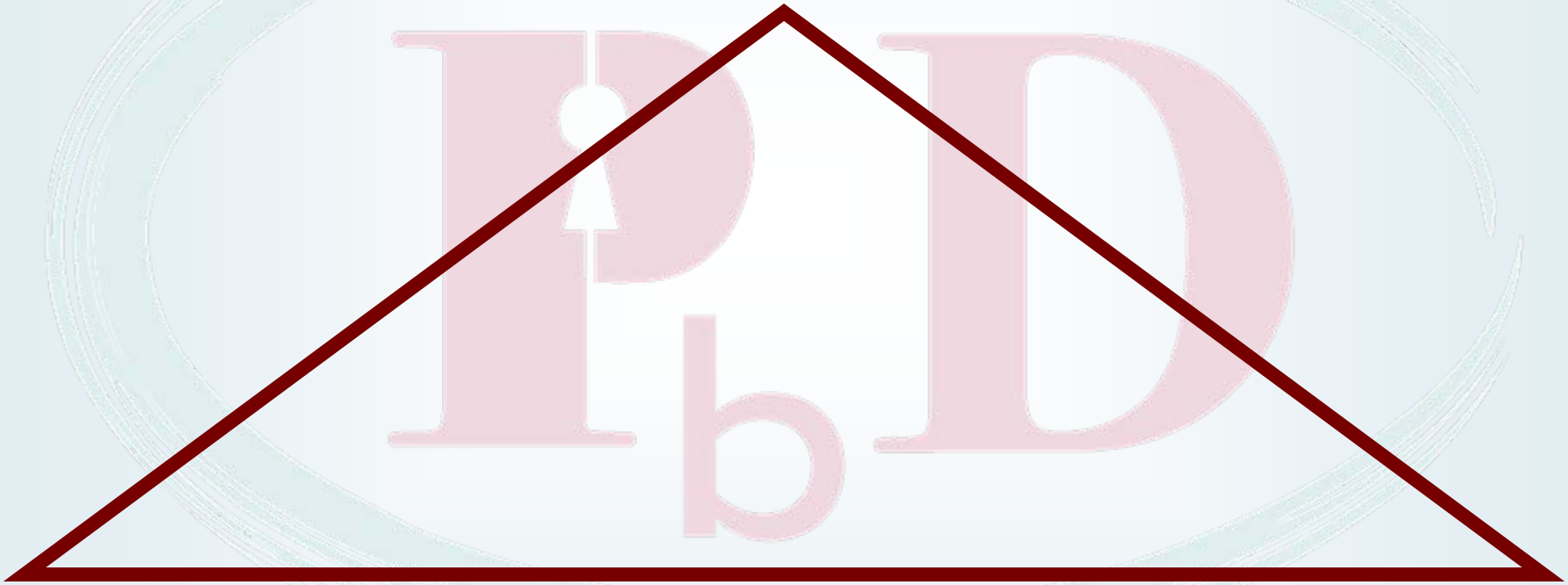
Toronto, Canada

November 17, 2010


PbD
www.privacybydesign.ca

Privacy by Design:
The Trilogy of Applications

Information Technology



Accountable Business Practices

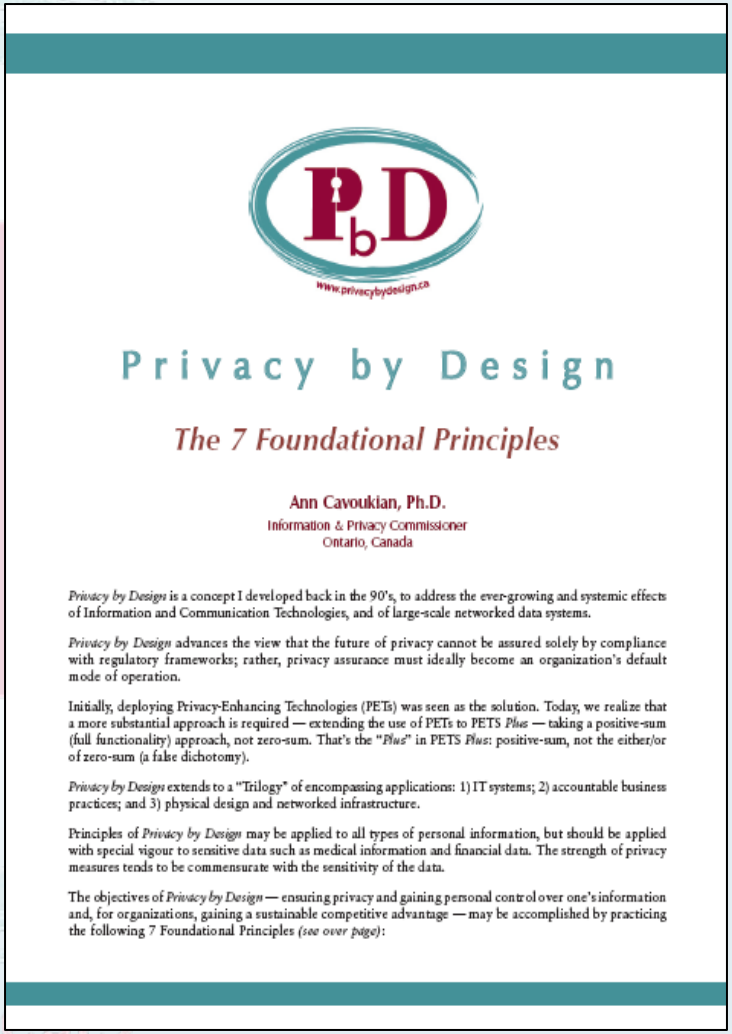
Physical Design & Infrastructure

Positive-Sum Model

Change the paradigm
from a zero-sum to
a "positive-sum" model:
Create a win-win scenario,
not an either/or
involving unnecessary trade-offs
and false dichotomies

Privacy by Design: The 7 Foundational Principles

1. ***Proactive*** not ***Reactive***:
   Preventative not Remedial;
2. Privacy as the ***Default***;
3. Privacy ***Embedded*** into Design;
4. ***Full*** Functionality:
   Positive-Sum, not Zero-Sum;
5. End-to-End **Security**:
   Lifecycle Protection;
6. Visibility **and** Transparency;
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).

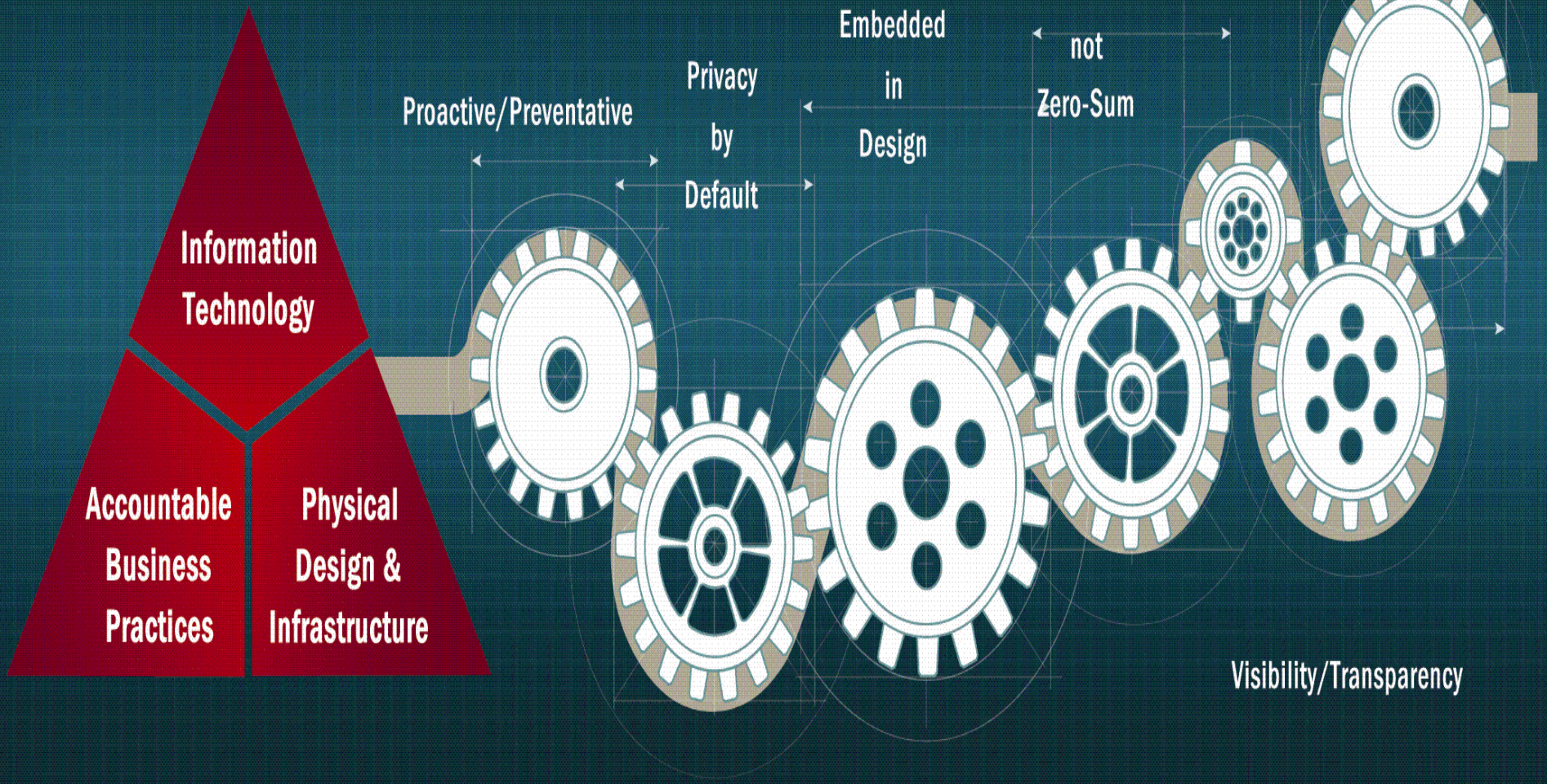
Privacy by Design extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure.

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.

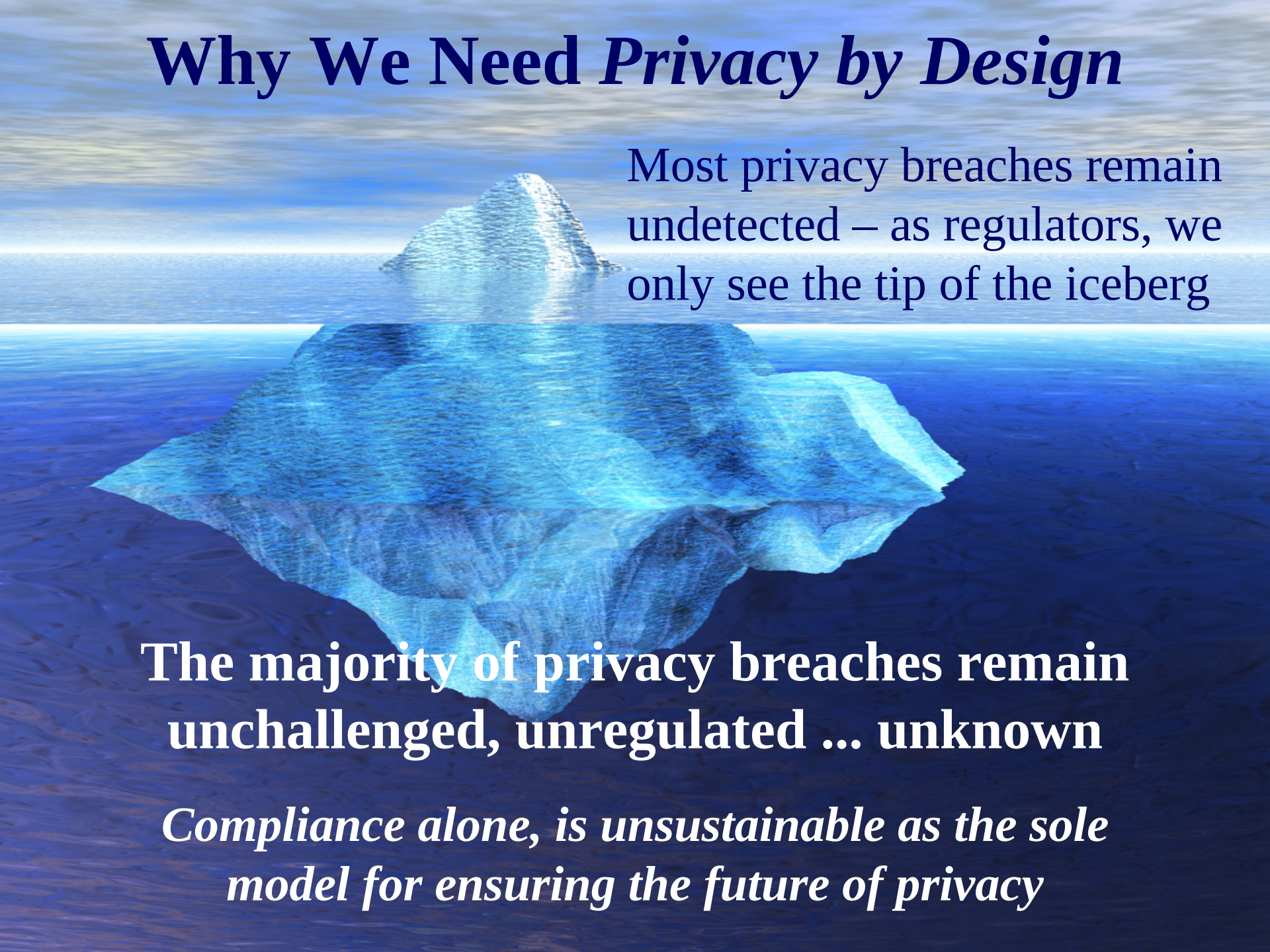
The objectives of *Privacy by Design* — ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following 7 Foundational Principles *(see over page)*:

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

Privacy by Design



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

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

Jerusalem – October 25, 2010

Smart Grid Privacy 101:
Privacy by Design *in Action*
Power Morning

Jerusalem

www.privacybydesign.ca

PbD

Smart Grid Privacy 101:
Privacy by Design *in Action*
Power Morning

Crowne Plaza, Jerusalem > Monday, October 25, 2010 > 8:00 – 10:00 a.m.

The Smart Grid presents new opportunities for growth and change. As well, it presents new challenges related to the collection of customer energy consumption data. Sophisticated utilities recognize the transformative nature of the Smart Grid and are taking steps to address the privacy issues that will inevitably arise. Their forward-thinking approach embraces the "Positive-Sum" principle of Dr. Cavoukian's *Privacy by Design* because it optimizes the interests of both electrical reform and privacy.

If you are a privacy regulator or professional, this two-hour seminar will provide you with tested, practical guidance enabling you to work with energy providers and utilities, ensuring the protection of personal information contained within the Smart Grid. Energy providers will also be interested to hear the first hand account of Hydro One's — Ontario's largest electricity company — implementation of a *Privacy by Design* Smart Grid.

Follow us at www.twitter.com/embedprivacy

Information & Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Canada

www.privacybydesign.ca

PbD

Dr. Ann Cavoukian
Information and Privacy
Commissioner of Ontario, Canada

Yoram Hacohen
Head of Israeli Law, Information
and Technology Authority

Adoption of "Privacy by Design" Resolution

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

TORONTO, October 29, 2010 /PRNewswire – 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.

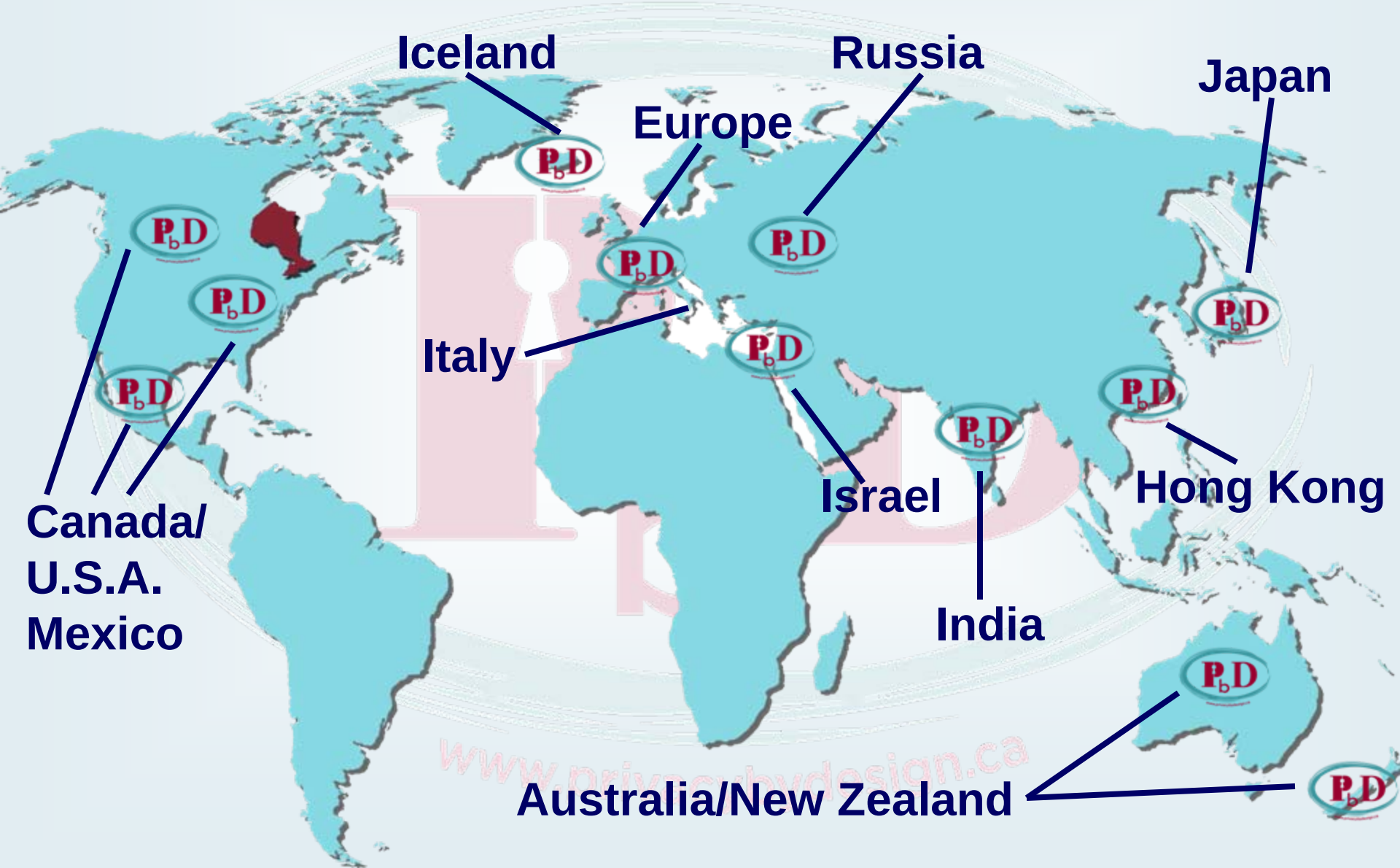
Full Article:

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

Adoption of "Privacy by Design" Resolution

- **October 29, 2010 –** regulators from around the world gathered at the annual assembly of International Data Protection and Privacy Commissioners in Jerusalem, Israel, and unanimously passed a landmark resolution recognizing *Privacy by Design* as an essential component of fundamental privacy protection:
  - Encourage the adoption of the principles of *PbD* as part of an organization's **default** mode of operation;
  - Invite Data Protection and Privacy Commissioners to promote *PbD*, foster the incorporation if its *7 Foundational Principles* in privacy policy and legislation in their respective jurisdictions, and encourage research into *PbD*.

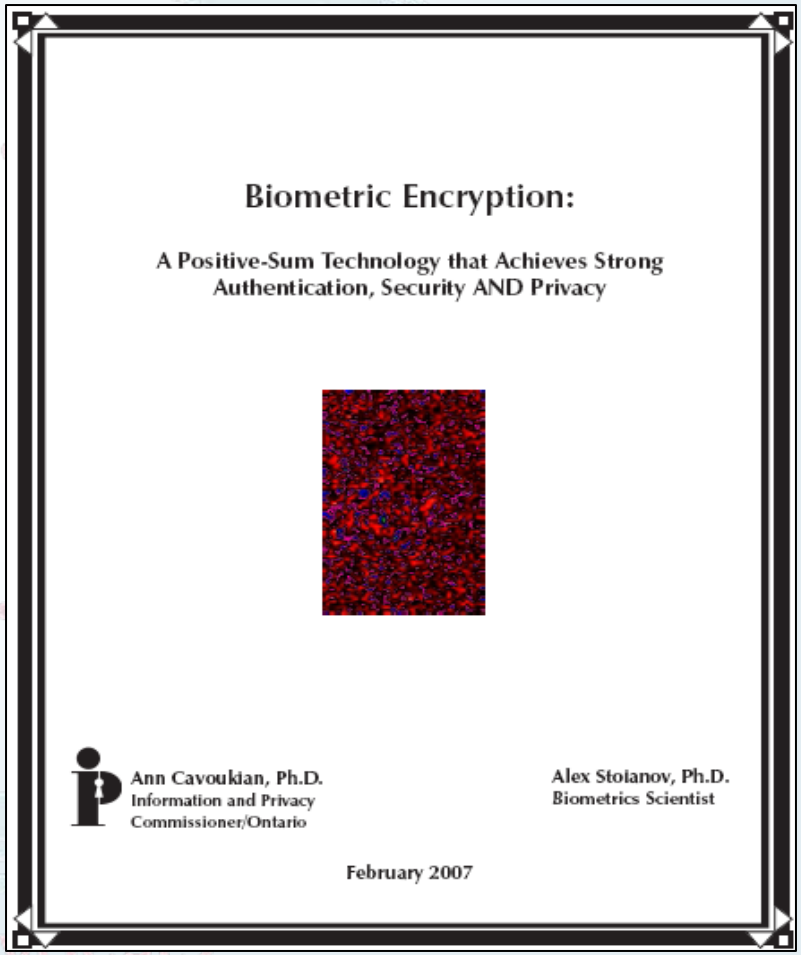
Privacy by Design – "Going Viral"



Privacy by Design
in Action

Biometric Encryption:
A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy

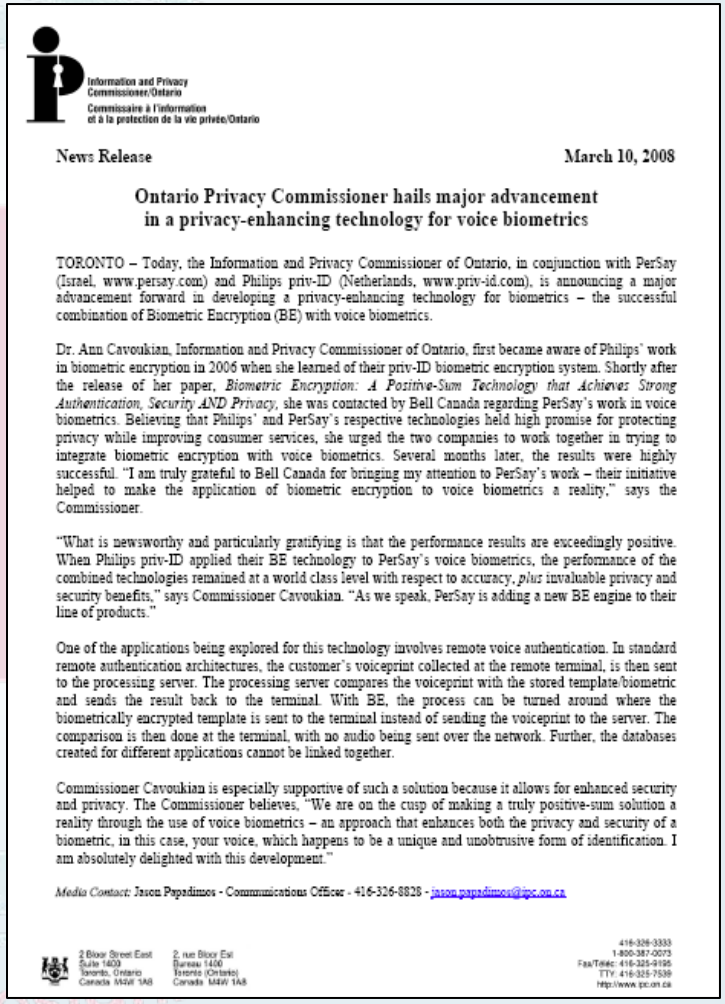
- Privacy-enhanced uses of biometrics, with a particular focus on the privacy and security advantages of BE over other uses of biometrics;
- How BE technology can help to overcome the prevailing "zero-sum" mentality by effectively transforming one's biometric to a private key.



www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf

PerSay
Voice Authentication Technology

PerSay (Israel)
– has successfully combined their own voice authentication technology with Philips' BE technology – a global first – making voice biometric encryption a reality!



Information and Privacy Commissioner/Ontario
Commissaire à l'information et à la protection de la vie privée/Ontario

News Release — March 10, 2008

Ontario Privacy Commissioner hails major advancement in a privacy-enhancing technology for voice biometrics

TORONTO – Today, the Information and Privacy Commissioner of Ontario, in conjunction with PerSay (Israel, www.persay.com) and Philips priv-ID (Netherlands, www.priv-id.com), is announcing a major advancement forward in developing a privacy-enhancing technology for biometrics – the successful combination of Biometric Encryption (BE) with voice biometrics.

Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario, first became aware of Philips' work in biometric encryption in 2006 when she learned of their priv-ID biometric encryption system. Shortly after the release of her paper, *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy*, she was contacted by Bell Canada regarding PerSay's work in voice biometrics. Believing that Philips' and PerSay's respective technologies held high promise for protecting privacy while improving consumer services, she urged the two companies to work together in trying to integrate biometric encryption with voice biometrics. Several months later, the results were highly successful. "I am truly grateful to Bell Canada for bringing my attention to PerSay's work – their initiative helped to make the application of biometric encryption to voice biometrics a reality," says the Commissioner.

"What is newsworthy and particularly gratifying is that the performance results are exceedingly positive. When Philips priv-ID applied their BE technology to PerSay's voice biometrics, the performance of the combined technologies remained at a world class level with respect to accuracy, *plus* invaluable privacy and security benefits," says Commissioner Cavoukian. "As we speak, PerSay is adding a new BE engine to their line of products."

One of the applications being explored for this technology involves remote voice authentication. In standard remote authentication architectures, the customer's voiceprint collected at the remote terminal, is then sent to the processing server. The processing server compares the voiceprint with the stored template/biometric and sends the result back to the terminal. With BE, the process can be turned around where the biometrically encrypted template is sent to the terminal instead of sending the voiceprint to the server. The comparison is then done at the terminal, with no audio being sent over the network. Further, the databases created for different applications cannot be linked together.

Commissioner Cavoukian is especially supportive of such a solution because it allows for enhanced security and privacy. The Commissioner believes, "We are on the cusp of making a truly positive-sum solution a reality through the use of voice biometrics – an approach that enhances both the privacy and security of a biometric, in this case, your voice, which happens to be a unique and unobtrusive form of identification. I am absolutely delighted with this development."

Media Contact: Jason Papadimos - Communications Officer - 416-326-8828 - jason.papadimos@ipc.on.ca

2 Bloor Street East, Suite 1400, Toronto, Ontario, Canada M4W 1A8 — 2, rue Bloor Est, Bureau 1400, Toronto (Ontario), Canada M4W 1A8
416-326-3333, 1-800-387-0073, Fax/Téléc: 416-325-9195, TTY: 416-325-7539, http://www.ipc.on.ca

http://www.ipc.on.ca/images/Resources/2008-03-10.pdf

Conclusions

- **Lead with *Privacy by Design;***
- **Change the paradigm from the dated "zero-sum" to the doubly-enabling "positive-sum;"**
- **Deliver *both* privacy AND security or any other functionality, in an empowering "win-win" paradigm;**
- **Embed privacy as a core functionality: the future of privacy may depend on it!**

How to Contact Us

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada

M4W 1A8

Phone: (416) 326-3948 / 1-800-387-0073

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

For more information on *Privacy by Design*, please visit:

www.privacybydesign.ca