Operationalizing Privacy by Design:

Guiding the Implementation of Strong Privacy Practices

Information and Privacy Commissioner,
Ontario, Canada

Estella Cohen
Executive Director

Friday, March 22, 2013

PRESENTATION OUTLINE

- Privacy by Design & 7 Foundational Principles
- How to ensure that a culture of privacy is developed and nurtured within the organization
- 7 Steps – From Policy to Operationalization
- Resources
- Questions / Answers

THE DECADE OF *PRIVACY BY DESIGN*

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

PRIVACY BY DESIGN:
PROACTIVE IN 30 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

- ***Cost-effective***
- ***Proactive***
- ***User-centric***
- ***It's all about control – preserving personal control over one's data flows***

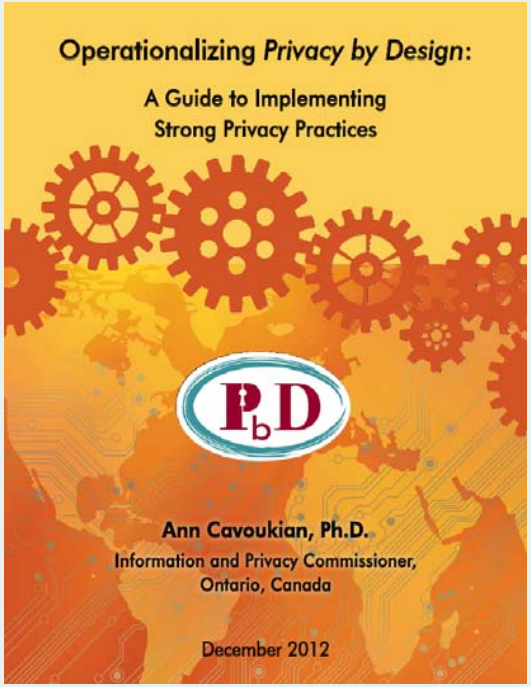
COMMISSIONER'S CORNER OPERATIONALIZING *PRIVACY BY DESIGN*:

http://www.youtube.com/watch?feature=player_embedded&v=5HTnyic2F0A

OPERATIONALIZING *PRIVACY BY DESIGN*

9 PbD Application Areas

1. CCTV/Surveillance cameras in mass transit systems;
2. Biometrics used in casinos and gaming facilities;
3. Smart Meters and the Smart Grid;
4. Mobile Communications;
5. Near Field Communications;
6. RFIDs and sensor technologies;
7. Redesigning IP Geolocation;
8. Remote Home Health Care;
9. Big Data and Data Analytics.



www.privacybydesign.ca

PRINCIPLE 1

Proactive not Reactive; Preventative not Remedial

Operational Guidance:

Anticipate and prevent privacy-invasive events ***before*** *they happen. Don't wait for privacy risks to materialize –* ***the aim is to prevent the breach from occurring.***

PRINCIPLE 2

Privacy as the Default Setting

Operational Guidance:

Seek to provide privacy assurance – delivering the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. ***No action should be required on the part of the individual user to protect their privacy*** *– it should be built into the system, automatically – by default.*

PRINCIPLE 3

Privacy Embedded into Design

Operational Guidance: *Embed privacy requirements into the design and architecture of IT systems and business practices.* ***Do not bolt them on as add-ons, after the fact.*** *Privacy should be an essential component of the core functionality being delivered.*

PRINCIPLE 4

Full Functionality – Positive-Sum not Zero-Sum

Operational Guidance: *Accommodate legitimate interests and objectives in a positive-sum, doubly-enabling manner, not through a zero-sum (win/lose) approach, where unnecessary trade-offs are made. Avoid the pretense of false dichotomies, such as privacy* ***vs.*** *security – substitute "and." Demonstrate that it is indeed possible to have both functionalities.*

PRINCIPLE 5

End-to-End Security – Full Lifecycle Protection

Operational Guidance: *Security is the key to privacy. Ensure cradle-to-grave, lifecycle management of information, end-to-end, such that at the conclusion of the process, all the data are securely destroyed, in a timely fashion.*

PRINCIPLE 6

Visibility and Transparency – Keep it Open

Operational Guidance: *Stakeholders must be assured that whatever the business practice or technology involved, it is, in fact, transparent to the user, and operating according to the stated promises and objectives, subject to independent verification.* ***Remember – trust but verify****.*

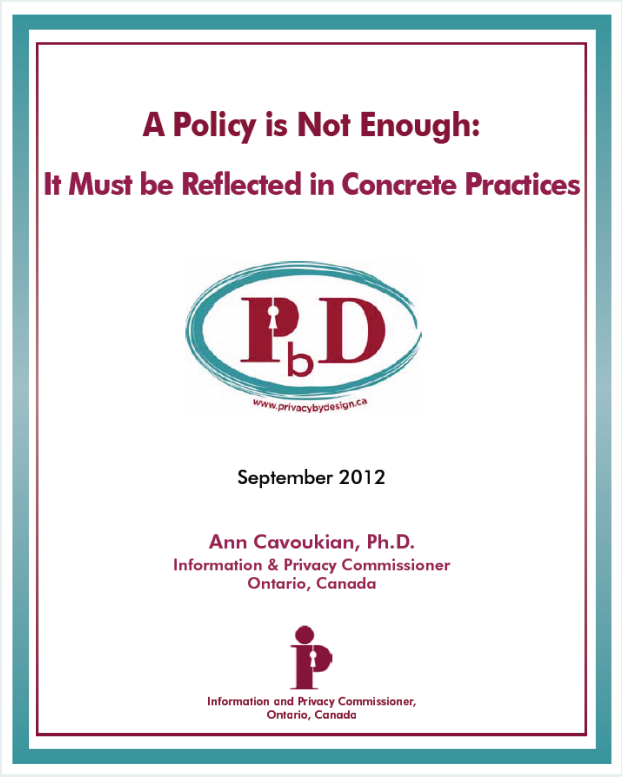
PRINCIPLE 7

Respect for User Privacy – Keep it User-Centric

Operational Guidance: *Architects and operators must keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice and empowering user-friendly options.* ***Keep it user-centric****.*

A POLICY IS NOT ENOUGH!

It Must be Reflected in Concrete Practices –
7 Steps to Taking Action



STEP 1

Implement a privacy policy that reflects the privacy needs and risks of the organization and conduct an effective Privacy Impact Assessment

STEP 2

Link each requirement within the policy to a concrete, actionable item – operational processes, controls and/or procedures, translating each policy item into a **specific practice** that must be executed

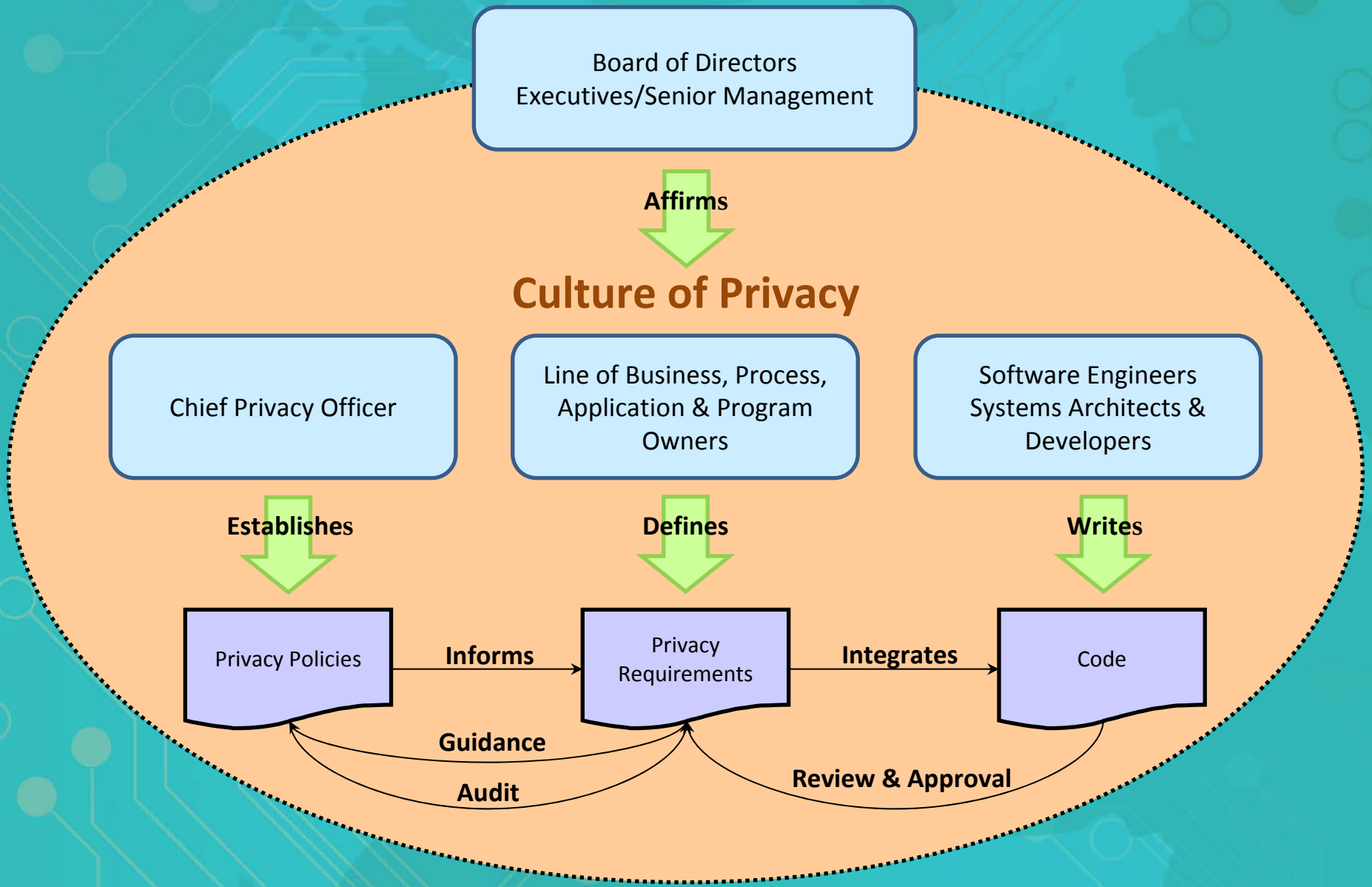
STEP 3

Demonstrate how each **action item** will then actually be implemented (as a regulator, I will be seeking evidence)

STEP 4

Conduct privacy education and awareness training to ensure that **all** employees (including those on the front lines) understand the policies/practices required, as well as the obligations they impose – and the need to act quickly

RESPONSIBILITIES



STEP 5

Designate a central “go to” person for privacy-related queries within the organization, preferably a Chief Privacy Officer

STEP 6

Verify both employee and organizational execution of privacy policies and operational processes/procedures – seek evidence of implementation (trust, but verify)

STEP 7

Proactively prepare for a potential privacy breach by establishing a data breach protocol to effectively manage a possible breach

CONCLUDING THOUGHTS

1. **Be proactive with privacy** – ensure that privacy is embedded in your systems and operational processes – into your business practices – don't let it be an afterthought;
2. **Policies are not enough**: It must be reflected in concrete practices;
3. **Save yourself money and resources** – it is far easier and more cost-effective to build in privacy up front; Get smart – get creative – innovate with *PbD*;
4. Embedding the principles of *Privacy by Design* will lead you to breach **avoidance**, thereby eliminating the need for breach notification.

Avoid Privacy by Disaster!

***For more information on Privacy by Design and* our full catalogue of publications, please visit:**

WWW.PRIVACYBYDESIGN.CA

CONTACT

Estella Cohen
Executive Director
Office of Information & Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario, Canada
M4W 1A8

Phone: 1-800-387-0073
Web: www.privacybydesign.ca
E-mail: info@ipc.on.ca

For more information on *Privacy by Design*, please visit: www.privacybydesign.ca