

Privacy by Design Research Lab

Dr. Marilyn Prosch, CIPP

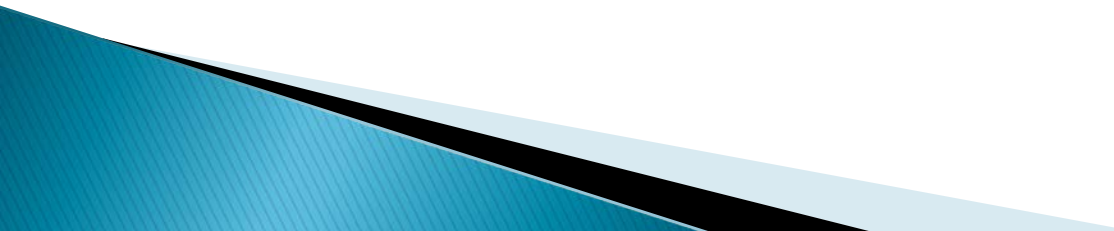
Dr. Ann Cavoukian

Privacy by **Re**Design

Mexico City
November 1, 2011



Privacy by Design


- ▶ Seeks to avoid breaches and their attendant harm, instead of offering various means of redress after the fact.
 - ▶ Originally conceptualized to circumvent the challenges that arise from treating privacy as an after-thought and attempting to “bolt it on” after the system had already been created.
- 

But....and this is a big butt...no pun intended

- ▶ We just can't throw out all new systems and start over, not practical.
- ▶ Work at **continuous improvement**.




And now introducing Pb^RD

- ▶ Privacy by **R**edesign
 - ▶ The concept of **data minimization** – the idea that the collection, use, disclosure and retention of personal information should be minimized wherever, and to the fullest extent, possible – underlies all of the PbD principles.
 - ▶ Unfortunately, many of the systems in existence today were designed under the **old philosophy** of more is better, because data storage is cheap.
- 

Paradigm Shift needed for discussing existing systems!

- ▶ These previously designed systems need to be updated to reflect the *paradigm shift from data hoarding to data minimization*.
- ▶ If you don't collect unnecessary data, you cannot lose it! Furthermore, organizations don't have to pay to protect it, this is certainly a win-win for business.
- ▶ Data minimization helps to ensure that privacy becomes the default condition throughout the system – the hallmark of an effective *PbD* implementation.

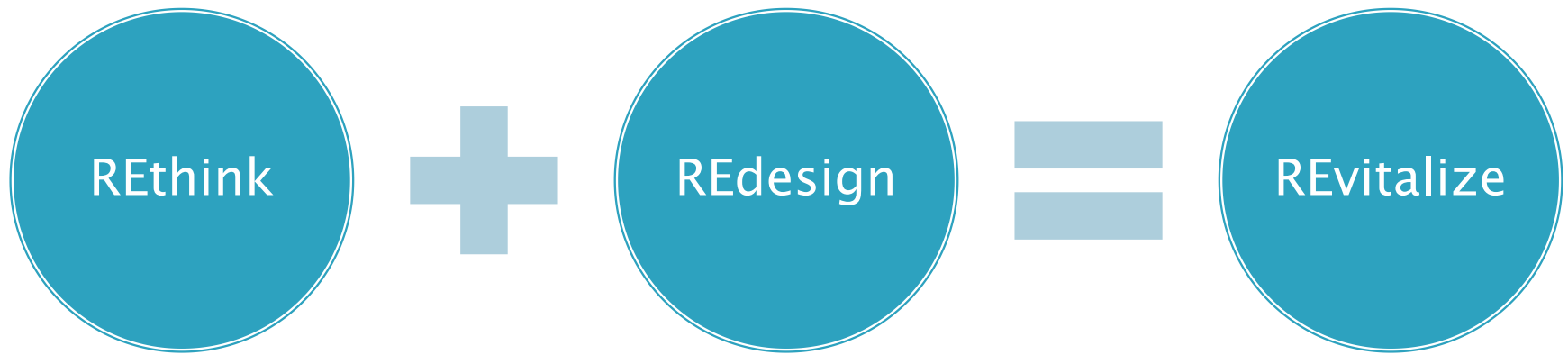
Business Systems are **ORGANIC**

- ▶ They evolve as a result of any of a number of factors, which may be generally grouped under the following categories:
 - ▶ **External Factors:** such as changes in legal requirements or industry best practices, and new partnerships or outsourcing arrangements (including cloud computing).
 - ▶ **Internal Factors:** such as ongoing risk management activities, technology upgrades, software modifications, changes in work processes or work flows; changes in work forces and expertise, changes in accountability and governance.
 - ▶ **Competitive Forces:** such as the need to build consumer trust and loyalty, the threat of new market entrants, changes in both supply and consumer demand, and opportunities to seize competitive advantages.
 - ▶ **Consumer Forces:** such as evolving user requirements, changes in customer expectations, and diversity of customer expectations in various global markets.
- 

Privacy by ReDesign – Pb^RD

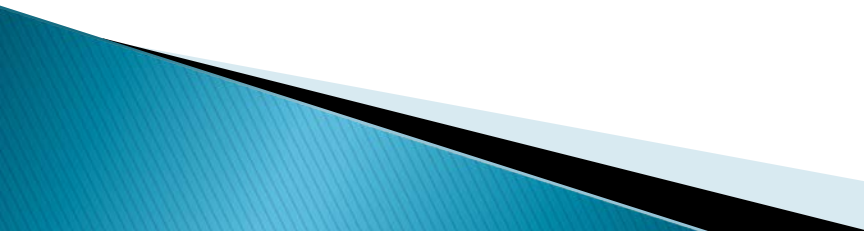
- ▶ *Privacy by ReDesign* is a new approach to applying the 7 Foundational Principles of *Privacy by Design* to existing systems: information technologies, business practices, physical design, and networked infrastructure.
- ▶ Clearly, since existing systems are already operational and pervasive throughout organizations, the principles cannot be embedded *from the outset*.

Instead, the objective must be to approach the end state of *PbD* – the highest standard of privacy protection – by seizing opportunities!

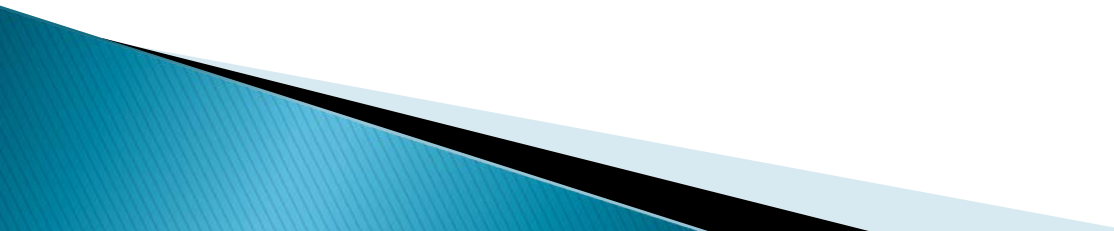


Pb^RD

Rethinking

- ▶ invites organizations to review their risk mitigation strategies, existing systems, and processes – including information technologies, business practices, physical design, and networked infrastructure – and consider alternative approaches that are more privacy-protective.
 - ▶ This may include revisiting assumptions about how much personal information is necessary for the system to operate, and how long it needs to be retained in identifiable form.
- 

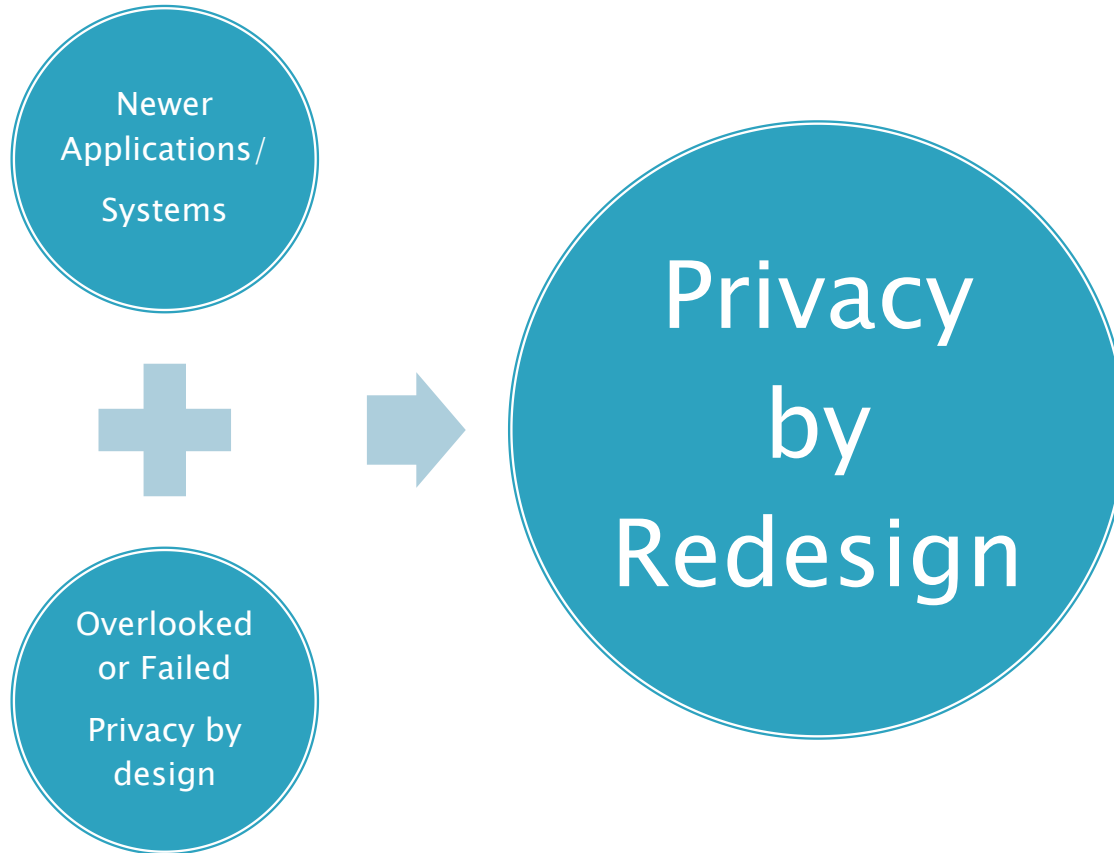
Redesigning

- ▶ represents the opportunity to enable or implement improvements in how the system functions from a privacy perspective, while also ensuring that it continues to achieve key business requirements in a doubly-enabling positive-sum, win/win relationship.
 - ▶ may likely require that less data is collected, and these changes may need to be cascaded back to stored databases where possible, to delete these unnecessary fields of data.
- 

Reviving

- ▶ the system in a new, privacy-protective way is the ultimate goal!

Just think about some of the newer systems growing rampantly...



A journey



- ▶ It will not happen overnight, but we'll never get there if we don't pack and go.
- ▶ Getting there can be both challenging and provide opportunities.
- ▶ Rest stops may be necessary, but we must persevere.

“Don't Stop Believing”
Journey