Privacy Engineering

A fresh proactive approach to privacy compliance

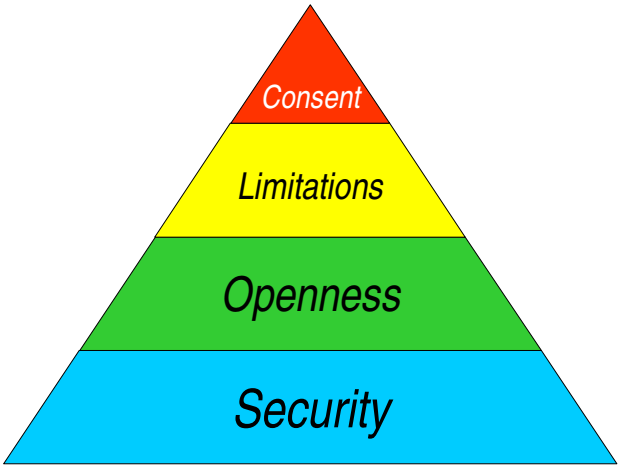
AISA Annual Seminar Day, Sydney, Nov 2007

Stephen Wilson
Managing Director
The Lockstep Group
www.lockstep.com.au

Privacy vs Security

- Privacy is framed as a human right
- Supreme Court Justice Louis Brandeis: *"The makers of our Constitution conferred … the right to be let alone – the most comprehensive of rights and the right most valued"* (1928)
- Security is "necessary but insufficient" for privacy

Privacy vs Security cont.



Attitudes to Privacy

"Privacy is not a technology issue"
Lou Gerstner, Chair IBM, 30 Nov 2000

This sort of simplistic slogan doesn't help anyone. Like all safety issues, protecting privacy involves a complex mix of technology, policy, legislation and education. To treat privacy as an education issue alone is like teaching road safety to adolescents but not worrying about seatbelts and speed limits.

Technology neutrality

No discrimination should be made among the various techniques that may be used to communicate or store information electronically

UNCITRAL Model Law on e-commerce

www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf

But tech neutrality has gone mad!

Clearly it has become quite fashionable to distance oneself from technology. An appalling number of important issues today are being disclaimed as having nothing at all to do with technology. But by dumbing things down, we only leave a bigger gap between "technology" and "the business", a gap in to which all sorts of privacy breaches can fall.

Political correctness!

"[A virus] is not a technology issue"
Microsoft spokesman to BBC, 2000

"Risk assessment … is not a technology issue"
CheckPoint at Senate Joint Committee, 2003

"I know that it sounds very basic, but education is the silver bullet"
Hani Durzi, eBay, New York Times, March 2005

"The biggest problem in solving phishing is that it is not a technology issue"
Network World Web Apps Newsletter Jan 2005

"Consumer id protection is not a technology issue"
Richard Hanson, VP RSA Security 2004

Perils of Tech Neutrality

"Technology neutrality is more a political buzzword than a clearly defined legal concept"

Technology Neutrality and Secure Electronic Commerce: Rule making in the age of "equivalence"
Michael Baum, Verisign 1999
www.verisign.com/repository/pubs/tech_neutral

Privacy Principles

IPP 1	Collection	**Don't collect info unnecessarily**
IPP 2	Use and disclosure	**Don't re-use info arbitrarily**
IPP 3	Data quality	**Care about the quality of info**
IPP 4	Data security	**Duh**
IPP 5	Openness	**Say why you need peoples' info**
IPP 6	Access & Correction	**Allows people to review & fix**
IPP 7	Identifiers	**Don't re-use other systems' ids**
IPP 8	Anonymity	**If practical, allow for anonymity**
IPP 9	Transborder flows	**Know others' privacy measures**
IPP10	Sensitive Info	**Extra care with health, race etc.**

Data collection

IPP 1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities

The Collection Principle is blind to the manner of collection. Don't fall into the trap of thinking it only applies to personal information expressly gathered through forms and questionnaires! There are five different ways most organisations collect personal information:

- ***Explicit*** forms, questionnaires
- ***Generated*** evaluative info (beware Basel II, AML)
- ***Automatic*** audit logs
- ***Acquired*** mailing lists, M&A
- ***Ephemeral*** help desk notes

Personal information inventory

Constructing an inventory held by an organisation helps it account for all personal information it holds, and prepare itself to safeguard that information in line with the law. Organisations need internal visibility as to how and why information is collected, and what happens to it throughout the personal information lifecycle.

WHAT All instances	**WHY** Specific reasons for collection	**WHERE** is info used? Map onto WHYs	**HOW** is it gathered?	**WHEN** is it gathered?	**WHO** else will see it?
1.	-	-			
	-	-			
	-	-			
2.	-	-			
	-	-			
	-	-			
3.	-	-			

Special topics

Without close and structured attention to privacy principles, the following activities and sub-systems can be especially problematic

- Database design
- Forms design & review
- Audit logs & transaction histories
- Portals & architectures
- Data destruction

Privacy & ICT: tensions

- Collection vs. generation
  Privacy laws don't care how personal information is collected, so don't forget to pay attention to internally generated data
- Audit logs testing vs. production
  Audit logging is important in testing and also production (where a paper trail is crucial for legal and business continuity reasons). However, don't forget that audit logs can create rich veins of personal information including subtle trails of what your users and customers have been doing (see next point).
- Transaction histories merit serious security
  Audit logs and transaction histories need to be designed and secured with the privacy principles in mind. Note too that technically under the law, customers also have a right to see and correct audit logs about them. Organisations should probably prepare themselves for these types of requests.
- Web forms not usually rigorously reviewed
  A commonplace channel for collecting customer information is the web form. Few organisations today "run a ruler" from a privacy perspective over web forms before publication. But if a form happens to ask for personal information without good reason – like the customer's home address or birth date, because it seemed like a good idea at the time – then the Privacy Act has been breached.

Privacy Engineering Guidelines

A new type of best practice guide that informs both ICT and "the business" at the formative stages of systems design, to make sure privacy is designed in, not simply retrofitted after compliance problems arise and the damage to customers and organisational reputation is already done.

- Privacy *is* a technology issue
- ICT practitioners need actionable guidance
- Benefits:
  - *Improve compliance position*
  - *Design privacy in to ICT projects*
  - *Reduce exposure to privacy breaches*