Lockstep Babystep No. 14

Introducing the concept of *Privacy Engineering*

The privacy Hall of Infamy

Scott McNally's quip that 'you have no privacy – get over it' usually tops the list of technologists' infamous privacy gaffs. But a more damaging viewpoint was revealed by a past chair of IBM, who affirmed that "Privacy is not a technology issue".[1] By positioning privacy as being apart from technology, this statement gives licence to technologists to ignore their own role in privacy, and perpetuates the sad cultural gap between technology and "the business".

What should privacy mean to technologists?

Many confuse privacy with security. The main difference is that privacy is all about *control*. No matter how secure a system may be, if it uses and discloses someone's information in unexpected ways, then it breaches their privacy.

Privacy is most certainly a technology issue, insofar as it can be influenced by IT practitioners. While formal responsibility for privacy usually rests with non-technology executives, privacy and IT intersect at a great many points. Technologists need to be alert to their role in minimising privacy impact. Therefore we coined the term "privacy engineering" in order to raise consciousness that more can be done to design privacy in at every point in the development lifecycle.

All Privacy Principles are impacted by IT

IT practitioners – indoctrinated with the falsehood that 'privacy is not a technology issue' – don't identify directly with many of the standard Privacy Principles. On their face, the new Unified Privacy Principles[2] only speak to technology in the area of security:

1. *Anonymity & Pseudonymity*
2. *Collection*
3. *Specific Notification*
4. *Openness*
5. *Use & Disclosure*
6. *Direct Marketing*
7. *Data Quality*
8. *Data Security*
9. *Access & Correction*
10. *Identifiers*
11. *Transborder Data Flows*

But all the UPPs are affected by how information systems are designed and built. All manner of inadvertent and non-obvious breaches can result from careless or ad hoc information flows. Moreover, non-technological privacy officers usually underestimate the extent to which IT determines compliance.

Classic privacy shortfalls

Technologists too often misjudge the **Collection Principle**. Privacy laws don't care how personal information is "collected", yet IT practitioners tend to think of collection only in terms of forms and questionnaires. The fact is that whenever *any* identifiable information comes to be in your system, by *any* means whatsoever, it is subject to the Collection Principle.

Audit logs often generate (that is, *collect*) personally identifiable information but are rarely secured to a standard commensurate with privacy regulations. Audit logging in the testing phase of a system should usually be wound back when it goes into production. It is dangerous to keep amassing detailed logs just because someone supposes that the data might be useful one day.

While systems designers tend to over-log the activities of customers, they sometimes *under-log* **third parties looking up customer data**. Because Use & Disclosure must be tightly controlled, it is vital that audit trails keep track of how personal information is accessed by others.

Too often, **questionnaires** composed by web masters ask for ad hoc demographic details. Unless the business needs to know a customer's age, gender, location and so on, it is not okay to ask. All web forms should be formally reviewed against the UPPs before going live.

Database schemas should be designed to anticipate the rights of individuals under privacy laws to access their records and request corrections. Producing a coherent and accurate snapshot of all information held on a named individual can be challenging in many organisations. Regulations require that 'notations' be made under various circumstances such as when a dispute over details cannot be resolved, and when special law enforcement related disclosures have been made.

[1] Lou Gerstner, Chair IBM, 29 Nov 2000; www-03.ibm.com/press/us/en/pressrelease/1464.wss.

[2] See www.austlii.edu.au/au/other/alrc/publications/reports/108/_4.html.