

Reflections on technology and privacy

Inaugural iappANZ Privacy Conference
Privacy in a Dramatically Changing Landscape
27 August 2008, Sydney

Stephen Wilson
Lockstep



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

Scott McNally's quip that 'you have no privacy, get over it' usually tops the list of technologists' infamous privacy gaffs, but a more insidious viewpoint is actually revealed by the previous chair of IBM. By positioning privacy as being apart from technology, he gives licence to technologists to ignore their own role in privacy, and perpetuates the sad cultural gap between technology and “the business”.

Political correctness!



The screenshot shows a Google search interface. The search bar contains the text "not a technology issue". Below the search bar, it says "Search: the web pages from Australia". The results section shows "Results 1 - 10 of about 14,900 for 'not a technology issue'". The first result is titled "Preventing data breaches not a technology issue - Network World" with a snippet: "When security people see headlines about data losses at TJ Maxx, ChoicePoint, DuPont, and the Department of Veterans Affairs, they quickly assume that ...". The second result is titled "Content Is Not a Technology Issue - ClickZ" with a snippet: "The wrong people are in charge of too many content projects. Content is not a technology issue".

It's actually entirely fashionable now to distance oneself from anything to do with technology. Only this week [25 Aug 08] the top hit went to the preposterous notion that data breaches is 'not a technology issue'. This is akin to saying that 'car safety is not a technology issue'.

Tech neutrality gone mad

"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

The truth is that all of these matters are really blended issues, and they have a great deal to do with technology. The ease with which slogans like 'privacy is not a technology issue' slide off the tongue indicates a malaise in which technologists badly underestimate their own impact on privacy.

Technology-privacy tensions



- **Collection vs. generation**

Privacy laws don't care how personal information is gathered, yet typical IT people tend to think of information gathering only in terms of forms and questionnaires.

- **Audit logs in testing vs. production**

Audit logs generate huge amounts of personally identifiable information and in many organisations represent a privacy disaster waiting to happen, as they are rarely secured to a standard commensurate with privacy regulations. Audit log requirements in the testing phase of an information system should usually be wound back when that system goes into production. It is not good enough to keep amassing detailed logs just because an IT person thinks the information might come in useful one day.

- **Web forms not usually reviewed against *PPs**

Too many times, forms composed by web masters include ad hoc demographic questions because they seemed like a good idea at the time. Unless the business needs to know a customer's age, gender or location, then it is not permissible to ask.

- **Transaction histories merit serious security**

Consider the fact that one can buy St Johns Wort online in the herbal remedy section of grocer shopping sites. There is only one use for St Johns Wort: self medication for depression. So the transaction histories of many otherwise innocuous e-commerce servers contain detailed indications of customers' mental health (or their perceived mental health).

Copyright © 2008 Lockstep Technologies Pty Ltd

Technological responses



- **Habitualise PIAs as a design tool**

Don't treat PIAs as a compliance or review tool; use them proactively at design time to uncover privacy issues and to help design privacy in

- **Improve identity protection**

It's high time that we started to treat IDs as seriously as we do car keys. Today our technology neutral stance admits a huge range of authentication techniques – passwords, one time logon generators, key fobs and even biometrics – most of which are known to be seriously deficient. We don't treat door locks or car locks with such disregard; neither should we treat our digital IDs so casually.

- **Embrace *identity plurality***

Deeper than any actual Privacy Enhancing Technology is the new privacy protective mindset of *Identity Plurality*, which recognises that we conduct our affairs in the real world according to discrete separate identities. When for example we do banking as an officer of a company, we are exercising a different identity compared to when we do personal banking. The best exposition of how this world view applies online is probably the Laws of Identity developed by Microsoft's Kim Cameron. This work has been abstracted and extended by Project Higgins. Identity Plurality is a subtly different and safer approach than the very popular Federated Identity movement, which too frequently morphs inadvertently into a single identity. Well meaning projects like OpenID have a tendency to naively collapse all digital persona into one master ID, making users even more vulnerable to phishing and ID theft.

Copyright © 2008 Lockstep Technologies Pty Ltd

Discussion



Stephen Wilson
www.lockstep.com.au

Copyright © 2008 Lockstep Technologies Pty Ltd

