From iappANZ Member Bulletin No. 12 (May 2010)

Google's wifi misadventure, and the gulf between IT and Privacy

This is the edited text of Stephen Wilson's column in the iappANZ members bulletin no. 12.

Everyone knows by now that privacy and security are not the same thing; *control* is the name of the game. Yet many responses to Google's most recent misadventure over wireless network data show we still have a long way to go. Too many are naively downplaying the incident as if privacy and *secrecy* are equivalent.

It's understandable for people to have a range of views about privacy. Not only is it personally felt, it is also a soft and multi-disciplined field, involving philosophy, human rights, civil liberties and politics. Yet *information privacy law* turns out to be rather clinical and is written to neatly sidestep philosophical and moral mine fields. This should make privacy law accessible to a wider audience, and yet its implications for IT remain misunderstood by many.

A few weeks ago it came to attention that Google Street View cars were collecting information from wireless networks they drove by. The extent of this collection wasn't clear at first, and speculation was confined to the seriousness of recording network names and device addresses transmitted publicly by wifi installations. In itself, basic network data is not identifying, but a nice privacy question arises if it can be linked to named individuals through Google's other vast data sets.

Google then revealed that their cars were also sampling regular data traversing unencrypted networks within range. Google explained that engineering software for an experimental wifi project was inadvertently included in the Street View system.

On blogs and discussion groups, many downplayed the collection of "public" data. Some blamed the victims, insisting that if network operators haven't taken care to turn on encryption, then their "broadcasts" are up for grabs. Yet carelessness does not equate to granting blanket consent for personal information to be collected and used for anything a technology company thinks of. Privacy law, like the Trade Practices Act, serves to protect the 'little guy' against exploitation by big business.

The critical legal point to me is crystal clear: information privacy law prohibits businesses from collecting personal information without an express need, or without consent, *whether the source data is in the public domain or not*.

When they learn about how the Privacy Act treats collection, many IT practitioners are incredulous, pointing out that vast volumes of information are generated and shared as a by-product of how networks work. And this fact of digital life does need to be understood by lawyers, legislators, policy makers, technologists and auditors.

Technical breaches of the Privacy Act probably occur all the time, by virtue of how computer systems operate, and in particular, how they tend to generate and hang on to log data.

A classic example is the personal data logged by e-commerce servers. Peoples' shopping habits represent personal information and e-merchants may fall foul of privacy law if they are logging transaction details without an express need. Worse, if the purchasing history includes medicines or even herbal remedies, then e-merchants are likely collecting *Sensitive Information*. Naturally customers' buying patterns can be an important marketing resource, but as such it can only be legally exploited if collected with consent and the primary purpose (i.e. marketing) has been made clear to all concerned.

Many organisations may find themselves in trouble if their technicians have enabled rich logging because they guess the information might be useful one day, without being specific and open about it. The engineer at Google appears not to have understood the Collection Principle, and I'm guessing that the culture at Google has not internalised the privacy principles in general.

Technologists especially should heed several lessons from the wifi misadventure:

— It might be counter-intuitive but publicly available information is still subject to information privacy law if it relates to identifiable individuals.

— Terminology matters (as technicians know in their own fields). The words "public" and "private" are not precise, so privacy law avoids them and instead is very specific about *personal information*

— Engineers must resist the tempt`ation to collect personal information just because they can.

— And software quality processes should include checks to see if excessive information collection is going on for whatever reason.

Copyright © 2010 Lockstep Consulting