The Devil wears the Emperor's New Clothes: technology, autonomy and the privacy myth

Eli Ball

Eli has recently completed a BCom (Accg)/LLB(Hons) at Macquarie University. In 2005 he took part in the Chicago based John Marshall Law School Moot Court Competition in Information Technology And Privacy Law. The moot explored several privacy and technology issues relating to the use of intrusive information technologies. His team placed 5th overall and was the top ranked International team. This article is based upon lessons from that experience.

As the push towards an Australian privacy tort gathers momentum, it is worthwhile reflecting on the impact such a development could have on the use of information gathering technologies. In this short article I argue that, based upon jurisprudence from the United States, the law of privacy could not and should not alleviate the responsibility falling on technology users to guard against invasions of their privacy. As information technologies become more pervasive, people should not expect the law to pick up the slack where they fail to take measures protecting themselves.

Lessons from the United States

A starting point for any discussion of privacy law is the United States Restatement (Second) of Torts. In particular, § 652B of the Second Restatement describes the four privacy torts: intrusion upon seclusion; appropriation of likeness; public disclosure of private fact, and; false light. Of these, it is the tort of intrusion that fits most neatly with the desire to protect a person's technological comings and goings. According to the Restatement, the tort is aimed at preventing those who intrude "physically *or otherwise*" into the private concerns of another. For example, if A wire-taps B's phone or spies upon him through a telescope an invasion of privacy is said to have occurred by virtue of A intruding upon B's seclusion.

There is, however, a major obstacle to consider when adapting the law of privacy to fit the technological exigencies of our time. That is the overarching requirement that a *reasonable expectation* of privacy must exist in the subject matter protected.[1] The decision of the U.S Supreme Court in *Kyollo v. United States* suggests that technology can play a major role in determining just what is 'reasonable' during times of technological change.[2] Kyollo was indicted for manufacturing marijuana after police discovered his indoor growing operation using a thermal-imaging device from the street. In his defence, he claimed that the thermal-imaging was an unreasonable search in violation of the Fourth Amendment to the United States Constitution. The Supreme Court agreed by a majority of 5:4. However, it added an important rider to its conclusion that the thermal imager was an 'unreasonable search'. Specifically, the majority stated that "it would be foolish to contend that... privacy secured to citizens... has been entirely unaffected by the advance of technology".[3] What saved Kyollo's appeal was the fact that the particular technology in question was not "in general public use".[4]

This suggests that, if a technology becomes pervasive enough, individual privacy rights surrounding it will in fact diminish. Individual privacy comes at the expense of public freedom and vice versa. As invasive technologies gain public acceptance and notoriety, the public expectation to protect the freedom fostered by that advancement will grow. Unless public concerns for privacy keep pace with technological developments the net result is an ever shrinking field of 'reasonable expectations' as people prioritise the freedom offered by technology over the protection of their individual rights.

Emphasising personal responsibility

If a privacy tort did emerge in Australia, the onus would fall on those claiming protection to take positive steps legitimising any expectation of privacy in the face of technologies that gain public acceptance and notoriety. Those who freely use the internet, for example, without guarding against the possibility of surreptitious spyware or cookies could not cry foul if their net-habits were observed by someone else. Similarly, those who subject themselves to an intrusive technology such as RFID tagging at a time when RFID readers are becoming progressively more common, would have their complaints for relief, fall on deaf ears without taking measures to guard against wayward or even intentional scanning by foreign parties.

The dangers these technologies pose to individual privacy are well known. The law should not have to intervene where a person voluntarily exposes themselves to that danger without taking the necessary precautions.

Consider the 'real word' example of a person entering a shop and being asked about their shopping habits. No one would claim that, after voluntarily providing an answer, the shopper was entitled to call an invasion of privacy. The situation is no different if the scenario takes place in an online setting and the relevant information is gathered via the use of a cookie ably placed on an unguarded and unprotected internet browser.

The key is to appreciate that technologies such as the internet pose nothing new in terms conceptual hurdles for the application and understanding of legal concepts. One may well remark that unlike the real world, an internet store has the ability to peer into the information we otherwise keep hidden from public

view on our computer. That, however, mistakenly assumes that such information is 'hidden' in the first place. Just because a person shops online in the physical privacy of their own home does not mean their venture into cyberspace is a private enterprise.

In the real world, when I walk into a shop, I am carrying all sorts of personal information from credit cards to family photos. They come into the shop with me, but are kept hidden because I choose to place them in my wallet away from public view. Using the internet, there is a cyber-equivalent to my wallet: namely, the use of software to guard against cookies, spyware and the like.

The reason I carry a wallet in the real world is that I know that if I didn't, people would be able to see my personal effects. The same is true of the internet: the proliferation of modes of spying on cyber-activities over the internet should not come as a surprise to anyone. In the same way I know the real world is full of people who can see me, I know that the internet is full of cookies and spyware. Just because there is no 'physical information' does not alleviate a person of the responsibility to guard their privacy through the appropriate medium.

Of course, where a person does go to reasonable lengths to protect their own privacy, only to have those efforts thwarted by some deviant or malicious application of technology, the situation is completely different. In those situations the expectation of privacy is a reasonable one and the law ought to intervene.

Conclusion: technology and the new public domain

It has been said time and time again in U.S. Courts that it is unreasonable to expect privacy from onlookers in a busy public place.[5] The same is true for a mass digital or online setting where physical onlookers are replaced with their well known technological equivalents. In the information age the application of new technologies has created a new public domain within which concerns for privacy need to be balanced. The law should not have to worry about protecting the privacy interests of people who voluntarily expose themselves to this new domain without regard for their own safety.

---

[1] See, eg, *Fletcher v. Price Chopper Foods of Trumann, Inc.*, 220 F.3d 871, 877 (8th Cir. 2000).

[2] 533 U.S. 27 (2001).

[3] Ibid, 35.

[4] Ibid.

[5] See, eg, *People for the Ethical Treatment of Animals ('PETA') v Bobby Berosoni Ltd* 895 P.2d 1269, 1279 (Nev. 1995).

A critical analysis of NSW procurement of ICT goods and services

Peter Mulligan

Peter Mulligan is a Senior Associate at Henry Davis York specialising in information, communications and technology law.

The NSW Government is a major purchaser of information and communications technology (**ICT**). It has an estimated annual ICT spend of $1 billion.[1] As such a big spender on ICT, it is a key customer to many suppliers.

The NSW Government market is also significant from a national perspective. Government is the single largest ICT customer in Australia. According to a recent study, within the government market, the NSW Government is the second largest customer behind the Federal Government.[2]

This puts the NSW Government in a unique position. Because of its spending power, it is able to shape and influence the development of the ICT industry in Australia. Depending on the areas in which it invests and the suppliers it awards contracts to, the decisions of the NSW Government have significant ramifications for the local industry.

It is an interesting time to be a supplier of ICT to the NSW Government. Last year saw the release of the NSW Government's new ICT Strategic Plan which sets the framework for ICT planning, expenditure and allocation of resources over the next 4 years.[3] The NSW Government has also begun using its new Procure IT terms and conditions for the procurement of ICT goods and services. Procure IT replaces the Government Information Technology Conditions version 2 which has been used by the NSW public sector since the 1990s.

ICT procurement policy is also evolving. In the last few years, the NSW Government has applied reforms to "provide a simplified, more predictable and accountable [procurement] process".[4] The Independent Pricing and Regulatory Tribunal has also recommended further reforms.[5]

Given the recent changes at the NSW Government level, it is a good time to take a closer look at the legislation, policies and contractual framework affecting the NSW Government market. The issues that will be touched on in this paper are the following.

1. The NSW ICT Strategic Plan
2. The legislative framework
3. The policy framework