

---

# 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.<sup>1</sup> 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.<sup>2</sup> *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".<sup>3</sup> What saved *Kyollo's* appeal was the fact that the particular technology in question was not "in general public use".<sup>4</sup>

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 world' 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