THE CONVERSATION

Academic rigour, journalistic flair

The challenge for legislators, courts and the wider community is to ensure any interference with privacy is minimal, rather than merely lawful. Shutterstock

Trust is the second casualty in the war on terror

May 10, 2018 6.25am AEST

This article is the second in a five-part series exploring Australian national security in the digital age. Read part one here.

Author

Bruce Baer Arnold

Assistant Professor, School of Law, University of Canberra

Contrary to doomsaying by pundits or empire-building by politicians and the surveillance-industrial complex, the so-called War on Terror doesn't mean we should – or must – kiss goodbye to our privacy.

It also doesn't mean we can forget the accountability of governments, officials and service providers. Nor does it mean we should abdicate responsibility for our own actions.

In thinking about terror and other aspects of national security, we need to consider how increased citizen surveillance affects our trust in government institutions and their private sector proxies.

Respect for privacy – essentially freedom from inappropriate interference – is what differentiates liberal democratic states from totalitarian states and terrorist groups. That respect is a fundamental value. It requires trust by ordinary people and officials alike that government and their proxies will abide by the law, remain accountable and not mistake what is expedient for what is necessary.

That trust has been eroded in recent years by the national security philosophy endorsed by both Labor and the Coalition.

The view from the bunker

National security policymakers and operatives, along with many privacy analysts, have a bleak view of the world. We recognise that Australia spies on friendly and unfriendly countries alike. They spy on us. That's a function of being a state. Non-state groups also seek to harm or gain advantages – that's not new.

The challenge for legislators, courts and the wider community is to look outside that bunker and ensure any interference with privacy is minimal, rather than merely lawful. At the moment, we are not doing well. It is unsurprising that law-abiding people are emulating Malcolm Turnbull by embracing privacy tools such as Wickr and Snapchat.

Lawmaking in Australia over the past two decades has involved a step by step erosion of privacy. The scale of that erosion has not been acknowledged by bodies such as the Office of the Australian Information Commissioner (OAIC), which consistently fails to rebuke bureaucratic opportunism.

Read more: The new data retention law seriously invades our privacy – and it's time we took action

---

The former Victorian Privacy Commissioner notably stood up to the premier and officials in his state, which is what we would expect from a privacy watchdog. Sadly, his willingness to speak truth to power was exceptional.

Protection against invasions of privacy has been progressively weakened in the name of "national security". This can be seen in the removal of restrictions on the sharing of information by agencies, pervasive biometrics such as the government's new facial recognition system and mandatory retention of telecommunications metadata. We see the militarised Home Affairs Department seeking to co-opt ASD - our most important spy agency - for warrantless access to the electronic communications of every Australian, rather than just 'hostiles' overseas.

Ongoing erosion cannot be justified. It has been persistently criticised by conservative bodies such as the Law Council of Australia and civil advocates such as the Australian Privacy Foundation.

Balances, not bullets

Privacy is not contrary to national security. It is a matter of balance, rather than an absolute.

Australian law (like that in the UK) has always allowed data collection, potentially on a mandatory basis – such as the Census. The law has always allowed overt or covert surveillance by officials, such as the undisclosed opening of mail or recording of conversations.

But such invasions must not be arbitrary. They must be restricted to those rare circumstances where disregard of privacy is imperative, rather than merely convenient. They must take place within a framework where there is some independent oversight to prevent abuse. Oversight fosters trust.

Such oversight might, in the first instance, consist of the requirement for a warrant, given our trust that courts will not rubber-stamp official abuses. It might involve systemic oversight by specialist bodies such as the Independent National Security Legislation Monitor (INSLM).

Asking the right questions

Australia does not have a discrete Bill of Rights under the national Constitution, although there have been cogent proposals from experts such as Bede Harris.

Privacy law is incoherent, with significant variation across states, territories and Commonwealth, and major holes in data privacy. Some states do not have a discrete Privacy Act, an absence that would be understandable in 1850, but is disquieting in 2018.

As a society, we expect officials will always do the right thing. Trust is fostered by laws that are necessary, transparent and properly implemented (for example, through the independent oversight noted above).

In thinking about these social objectives – more than just "winning" a conflict that may last across generations – we need to ask some hard questions about public and private responsibility.

Read more: How the law allows governments to publish your private information

---

The first question we must ask, as citizens, is whether privacy - and law - is something that should always be sacrificed when there is a perceived threat to national security. We should acknowledge that not all threats are equally serious. We need informed public discussion about the need for and appropriateness of governments restricting use of private encryption tools and requiring that service providers offer law enforcement officials secret back doors into private communications.

Another question is whether officials should access private communications simply by asking service providers, without the discipline provided by a warrant. Can we tell if there have been abuses of our privacy? Watchdogs such as the OAIC and the INSLM need stronger protection from political pressure) and more resources, on the basis that an underfed and frightened watchdog is ineffective.

What's more, we need to question to what extent we should trust governments and officials that are hostile to public disclosure. This hostility is exemplified by the Commonwealth Public Service Commissioner's characterisation of FOI as "very pernicious" and the two years the OAIC spent in budgetary limbo, following efforts by the Abbott government to shut it down.

There are times when it is in everyone's interests not to share secrets. That isn't always the case, and we must ensure our governments, which exist to serve us, are accountable.

Privacy National security War on Terror Data privacy Global perspectives