Irresistible Urges: Surveilling Australia's Citizens

By Dr. Binoy Kampmark
Asia-Pacific Research, May 03, 2018

Region: Oceania
Theme: Politics, Society

The authoritarian misfits in the Turnbull government have again rumbled and uttered suspicions long held: Australian residents and citizens are not to be trusted, and the intelligence services should start getting busy in expanding their operations against the next Doomsday threat.

This became clear from leaked material on discussions that illustrate in no subtle way the security paranoia afflicting officials in the nation's various capitals. A merry bunch they are too, featuring the Home Affairs Minister **Peter Dutton** and his advisor and department secretary, **Mike Pezzullo**. These latest discussions disclose not so much a change of approach as a continuation of a theme the Australian national security has taken since 2001: we are menaced constantly, and need the peering folk and peeping toms to pre-empt the next attack, fraud or swindle.

Central to the latest security round robin is a familiar, authoritarian theme: the Australian Signals Directorate (ASD) should be given access to emails, bank records and text messages without the knowledge of citizens, tantamount to a data home invasion. A mutual role would thereby be cemented between defence and home affairs.

Minister Dutton has found it hard to contain his delight at the prospect of further influence, despite rejecting the notion that his moves would lead to carte blanche espionage on home soil. According to the ABC, which has attempted to make sense of the latest chatter, the ASD would be given a larger role on three levels.

The first would involve deploying shutting down or "cyber effects" powers against the usual gifts that keep giving alibis: organised criminals, child pornographers and terrorists. "Penetration tests" on Australian companies to test the value of their cyber security against hacking would also be conducted. The third arm of enlarged power would entail giving the ASD powers to coerce government agencies and companies to improve cyber security.

Over the weekend, the secretaries of Defence, Home Affairs and the ASD issued a joint statement claiming that the latter's "cyber security function entails protecting Australians from cyber-enabled crime and cyber attacks, and not collecting intelligence on Australians."

The secretaries insist on a scrupulousness that barely computes:

> "We would never provide advice to Government suggesting that ASD be allowed to have unchecked data collection on Australians – this can only ever occur within the law, and under very limited and controlled circumstances."

The state of protections citizens have is hardly rosy as it is: ASIO is tasked with the issue of conducting espionage on Australian territory though it needs warrants signatured by the Attorney General. The Australian Federal Police also require warrants. The ASD, to date, been a helper rather than a controller, a two-bit player and data cruncher.

Not all ministers are on board with the plan, notably the **Foreign Minister Julie Bishop** (image on the right). A palpable shift of power is taking place in the bureaucratic machinations of Canberra, and the suggestions that the ASD be given enhanced powers to produce intelligence on Australians suggests a further circumvention if not outright evisceration of the Attorney-General's department.

Dutton and his cadres are also mounting an offensive on other surveillance fronts, something typified by the weasel language of the "central interoperability hub". The Home Affairs department already shows sign of bloating self-importance, floating more ideas about how best to keep the large eye of the state attentive to security threats. A facial recognition system, for instance, is on the table, and is likely to be given the blessing of parliament.

The Law Council of Australia has reason to worry as, for that matter, does everybody else. Giving government agencies the means to identify a face in a crowd can only have a broadening effect, resulting in prosecutions for minor misdemeanours.

On this score, the governments of the states and territories are with the Home Affairs department, having agreed in October last year to the sharing of identity and facial recognition data between all levels of government to target the usual bogeys that threaten Australia's cobbled civilisation: organised crime, terrorism and identity fraud.

The surveillance sorcerers, it would seem, are rampant, a point made clear in the *Identity-matching Services Bill 2018*. This potentially insidious bit of drafting "provides for the exchange of identity information between the Commonwealth, state and territory governments by enabling the Department of Home Affairs to collect, use and disclose identification information in order to operate the technical systems that will facilitate the identity-matching services envisaged by the IGA." (Crypto-authoritarians tend to be rather verbose.)

The Bill's wording also abhors the state of current image-based methods of identification, these being "slow, difficult to audit, and often involve manual tasking between requesting agencies and data holding agencies, sometimes taking several days or longer to process". The travails of a liberal democracy, ever a nuisance to those protectors citing omnipresent threats.

The Council's president, **Morry Bailes**, has already hammered out the words he intends to tell the parliamentary joint committee on intelligence and security:

> "Clearly, provision of such capability has been desirable to facilitate detection of would-be terrorists scoping a site for a potential terrorist attack. But that very same identity-matching capability might also be used for a range of activities that Australian citizens regard as unacceptable."

Even Bailes effuses pieties, thinking that clearly drawn lines on the use of such data will somehow save the sacred cow of civil liberties. (That cow, it must be said, is in a poor state of health as it is.) He insists on such canons as legitimate use and proportionality, two features managers of the national security state are inherently incapable of.

> "That line should also be assured by law to be fully transparent, understood and consistently applied by all relevant governments and their agencies."

But such a line might creep, advancing "towards broad social surveillance" finding its way "to a full social-credit style system of government surveillance of Australian citizens."

The issue common to the latest pro-surveillance bingers is an innate desire to remove the judicial arm from the equation. Having a warrant takes time and resources; leaving surveillance to the discretion of state officials is far more expedient and tidy.

As the Australian Human Rights Commission notes, the "very broad powers" granted to Dutton as Home Affairs minister "could lead to further very significant intrusions on privacy." There are no discernible "limits on what may be done with information shared through the services the bill would create".

The latest ASD affair, with other surveillance agendas in the wing, suggests that a very unfitting eulogy for Australian civil liberties is being written. Authoritarianism is being kept in check by ever weakening forces and fetters. The insecurity of citizens is deemed a suitable price for the security of the state – just the way Dutton likes it.

*

Dr. Binoy Kampmark *was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. He is a frequent contributor to Global Research and Asia-Pacific Research. Email: bkampmark@gmail.com*

Articles by: **Dr. Binoy Kampmark**