Australian Citizens Party

Craig Isherwood, National Secretary
PO Box 376, COBURG, VIC 3058
Phone: 1800 636 432 **Email:** info@citizensparty.org.au **Web:** citizensparty.org.au

MEDIA RELEASE

4 October 2018

Don’t let the Five Eyes spy on you!

If the Australian government’s latest anti-terror bill passes, sometime in the not-too-distant future you could find yourself unwittingly relaying a trail of personal information and your day-to-day activities to Australia’s security agencies. And you would be none the wiser. The Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 will allow spy agencies like the Australian Security Intelligence Organisation (ASIO) to hack into your electronic devices, by making app or software providers, chat rooms and the like re-engineer your programs, allowing them to bypass encryption protocols without your knowledge. And that is just one of the new mechanisms these agencies will have to spy on you. (Read more in “Home Affairs encryption bill: A political tool made in Britain”, *AAS* 5 Sept.)

Of course we are assured by the government that the new provisions are intended only for “criminal syndicates and terrorists” and that there will be “robust safeguards” in place to prevent their misuse. The rush to pass the bill with as little scrutiny as possible, however, indicates otherwise.

The bill was released to the public on 14 August and tabled 20 September. In a brief consultation period after the draft bill’s release, 15,000 submissions were received. Once tabled, the bill was referred to the Parliamentary Joint Committee on Intelligence and Security, but only a three-week submission period was scheduled. Why is the government in such a hurry to ram this through?

In his 20 September speech introducing the bill to parliament, Minister for Home Affairs Peter Dutton admitted that “The bill provides law enforcement agencies with additional powers for overt and covert computer access. Computer access involves the use of software to collect information directly from devices”, he said. But, he insisted, it is “not a new vehicle to collect personal information”.

Dutton claimed the security agencies’ lack of access to encrypted communications presents a significant barrier to combating national security threats. The uptake of “encrypted communications platforms by criminal and terrorist groups has been sudden. It represents a seismic shift….” This has interfered with ASIO’s ability to spy, he reported.

A Five Eyes play

The legislation did not emerge out of thin air—it is a copy of a UK law passed in November 2016, the I*nvestigatory Powers Act* (IPA), a.k.a. the “Snoopers’ Charter”. The Australian bill contains a variation of the UK bill’s mechanisms: technical assistance notices which compel service companies to provide assistance, and technical capability notices which require a company to take reasonable steps to develop and maintain a capability to respond to security agency requests.

The UK law allows companies to violate existing laws in order to comply with the notices, and it has been suggested that agencies could compel not only internet service providers, email servers and telcos, but any organisation, from a business to a hospital or political party, to collect information on behalf of the government. The UK Parliament is currently debating another new law, the Counter-Terrorism and Border Security Bill 2017-19, which former MI5 officer Annie Machon has described as a move towards a “techno-Stasi state”. Under the legislation, classified information would be shared with the private sector, councils, schools or social workers to enhance spying capabilities. Another provision would allow police to close the entire “Square Mile” City of London banking centre to foot and vehicular traffic in the event of an emergency, terrorist *or economic*.

Australia has been a leading nation in the Five Eyes’ push for a new standard of state-secrecy to prevent so-called foreign interference, with the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* passed on 28 June. Upon its passage, independent federal MP Andrew Wilkie warned that Australia is a “pre-police state”; but the Five Eyes spying alliance, comprising the USA, UK, Canada, Australia and New Zealand, has even bigger plans. As Home Affairs Secretary Michael Pezzullo revealed prior to the Five Country Ministerial meeting held 28-29 August on the Gold Coast, the Five Eyes countries are pushing for a global police-state capability , with a “transnational model of security”.

The real agenda is also betrayed by the fact that British authorities have freed 500 terrorists from prison since the 11 September 2001 terrorist attack in the USA; increasing to approximately one per week over the year to March 2018. Despite the relentless wave of new anti-terror laws, the

government claims it is powerless to stop these releases. In reality, it is well documented that British security services have maintained a covenant with terrorists, allowing them to operate from the UK.

Terrorism and foreign interference are being used as pretexts to implement police-state controls that will be used to protect establishment interests, as the economy sinks further into crisis and the population revolts against measures such as "bail-in" laws that will seize the savings of ordinary people to prop up the failing financial system.

Opposition to the bill

The proposed Australian powers are broad and will be exercised in secret, so there can be no real oversight outside of the agencies deploying them and the Attorney General's department. The penalty for citizens disclosing information about operations is five years' imprisonment; for not complying with an assistance order, 5-10 years! This is an effective weapon against potential whistleblowers. We already have the example of "Witness K"—the former Australian Secret Intelligence Service officer facing two years in prison for rightly exposing how the Australian government spied on the East Timorese cabinet during negotiations over an oil and gas treaty in 2004.

The brief period of feedback for the draft bill, though not advertised, attracted a great deal of criticism. Of the 15,000 submissions, 14,300 were generated by a Digital Rights Watch campaign, which is indicative of the public dissent. The Australian Human Rights Commission exposed the "breadth of the powers, the ambiguity of certain provisions and the inadequacy of effective safeguards"; Australian Lawyers for Human Rights said the Bill seriously impinges on human rights and "limits the presumption of innocence by allowing covert access to personal communications and criminalising the refusal to share one's passwords".

Human Rights Watch said the bill would set a dangerous precedent worldwide and that its ambiguities and broad powers could introduce "widespread security vulnerabilities", a concern also raised by the Australian Industry Group, the Communications Alliance and the Digital Industry Group. The Labor Party slammed the "sham" consultation process and the rush to table the bill within ten days of submissions closing.

Submissions to the Parliamentary Joint Committee can be made at www.aph.gov.au/Parliamentary_Business/Committees/OnlineSubmission by noon on 12 October.

Printed from http://citizensparty.org.au/print/pdf/node/370, on 21 Jul 2024 at 01:07 am