Identify and Disrupt: Australian police-state law #92

A bill to provide even more extraordinary powers to intelligence agencies to spy on Australian citizens, originally tabled in December 2020, was rushed through the Australian Parliament in August. The *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* is supposed to identify and disrupt threats to the safety of Australians. But while the intrusive new powers were deemed necessary to combat "serious crimes", including child abuse and exploitation, terrorism, human and drug trafficking, identity theft and fraud, assassination and weapons distribution, they in fact apply more broadly to other crimes as well. Since the 11 September 2001 US terrorist attack, at least 92 new and far-reaching national security laws have been passed in Australia, all of which create new crimes from already existing ones by couching them in terms of new, vague categories of terrorism or cyber-crime.

In late 2019 the Home Affairs Department launched a push for new powers to prevent a "cyber Pearl Harbor". The new powers would help police the largely unregulated world of the internet, the story went, despite the fact that existing law, namely the *Intelligence Services Act 2001*, already enabled the Australian Signals Directorate (ASD) to intervene, with Ministerial authorisation, on an emergency case-by-case basis to prevent "serious crimes" involving the movement of money, goods or people, transmission of data, or the use or transfer of intellectual property. ("Pezzullo hypes 'cyber Pearl Harbor' in push for more police-state powers", *AAS*, 6 Nov. 2019.)

Similarly, the latest law hands new powers to the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC). According to a review of the *Identify and Disrupt Act* for Michael West Media by barrister and Australian Lawyers Alliance spokesman Greg Barns, the new law works this way: "An AFP or ACIC officer 'may apply to a judge or a member of the Administrative Appeals Tribunal' for what is called a 'data disruption warrant'. This means the officer can add, copy, delete or alter data held in the computer."

A warrant is granted on the basis of "reasonable grounds" of suspicion, for any offence "likely to be" committed or if disruption of data is "likely to substantially assist" prevention of the offence, says Barns. Additionally, if time to obtain a warrant is lacking, it can be immediately granted, with the affidavit justifying its use delivered up to three days later.

One type of warrant allows an AFP or ACIC officer to take control of online accounts of private citizens in order to obtain evidence of the commission of an offence. As Barns points out, this "could lead to the destruction of exculpatory data, the manipulation of data, and the unlawful sweeping up of 'evidence' that is unrelated to the warrant; or even remove what may be used as proof of innocence", or entrapment of individuals.

"Australia does not have a national human rights charter or law", states Barns, and this bill is a step towards the opposite outcome—enshrining human rights violations into Australian law.

Where's the opposition?

An inquiry by the Parliamentary Joint Committee on Intelligence and Security chaired by Senator James Paterson did not propose any material changes to the bill, only recommending adequate oversight and review, and proportionality in use of powers. The final report of the committee stated: "The Committee accepts evidence the threat environment from serious cyber-enabled crime is severe and Australian authorities do not currently have the tools to address the threat."

While acknowledging that the powers sought were "extraordinary", the Labor members on the committee supported the report, and, like all previous policing powers, waved them through when they hit the Parliament. In the brief debate prior to the bill's passage, Labor Senator Kristina Keneally only demanded the powers be used proportionally and agencies be alert to "surveillance creep" between the serious crimes it is justified by, compared with actual usage.

In its submission to the inquiry the Law Council noted that, despite the suggestion in the Explanatory Memorandum that the proposed amendments were minor, they were in fact significant in that they authorised law enforcement officers and other covert operatives to engage in activities that would otherwise constitute offences or torts (including such things such as the dissemination of a computer virus), and the limiting of a court's discretion to exclude evidence on the basis that it was unlawfully or improperly obtained. The Law Council further expressed the view that the existing provisions in the *Surveillance Devices Act 2004*, which the bill amends, were a carefully designed safeguard which already took into account the issues identified in the Explanatory Memorandum as warranting the Bill.

Already super cyber capabilities

With the upsurge in concern over new digital and cybercrimes, a whole roster of new agencies has appeared in recent years. The 2016 Defence White Paper and 2016 Cyber Security Strategy established: the Australian Cyber Security Centre at the ASD; Joint Cyber Security Centres in most state capitals to work with industry; a 24/7 Global Watch body to respond to critical cyber incidents; and an Information Warfare Division within the Australian Defence Force, which includes a cyber unit

with responsibility for defensive and offensive cyber operations. The Australian Strategic Policy Institute (ASPI) also hosts an International Cyber Policy Centre that receives funding from the ASD and tech companies like Microsoft, Amazon, Facebook and Google. In addition, the Australian Prudential Regulation Authority (APRA) has been working with the world's top intelligence agencies to combat cyber-attacks, including by monitoring aggregated private financial data.

The 2020 Cyber Security Strategy, with its Cyber Enhanced Situational Awareness and Response (CESAR) package, increased funding and added five hundred extra ASD spies, a new cyber threat-sharing platform, and new research and intelligence capabilities. ("Spies on the rise as nation gets battle-ready", *AAS*, 15 July 2020.)

A number of other recent laws allow interception of online activity. These include the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, which allows intelligence and law enforcement agencies unprecedented access to the private data of citizens ("Don't let the Five Eyes spy on you! ", Media Release, 4 October 2018); and the post-Christchurch attack legislation to prevent sharing of terrorist acts on social media, the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019*, which experts warned could suppress whistle-blowers and censor media content. ("'Christchurch Call' establishes dangerous pretext for state censorship", Media Release, 28 May 2019)

Whole new categories of crimes are being created before our eyes. In reality, the crimes are the same, but the fact that communications regarding them are conducted over a new medium is providing a sham pretext for broad, new abrogation of freedoms.

By Elisa Barwick and Bob Butler, Australian Alert Service, 15 Sept. 2021
