

Australian government moves to boost data-swapping with US spy network

Mike Head
9 March 2020

The Australian government is helping spearhead moves by the Trump administration to force internet companies to hand over encryption-cracking capabilities, and to intensify data-swapping within the US-dominated “Five Eyes” global surveillance network.

At a Five Eyes summit in Washington D.C. last week, Australian Home Affairs Minister Peter Dutton joined US Attorney General William Barr and senior ministers from the UK, Canada and New Zealand in ramping up their demands that the tech companies provide unprecedented access to their customers’ encrypted communications.

At the same time, in Canberra, the Liberal-National Coalition government unveiled a bill to expand and legalise the capacity of the US intelligence and police agencies, including the National Security Agency (NSA), to obtain intercepted data from their Australian counterparts, and vice versa.

This dual development highlights the frontline role being played by the Australian government and military-intelligence apparatus in the mass spying operations and war preparations of the US authorities.

As the thousands of secret US documents published by NSA whistle-blower Edward Snowden and by Julian Assange via WikiLeaks showed, the Five Eyes partners intercept the communications of millions of people around the globe, routinely exchange data about each others’ citizens, and also supply cyber warfare facilities and targeting information to their militaries.

Both Barr and Dutton dressed up the intensified collaboration as one focused on combatting on-line paedophilia. Dutton hailed “a new page” in the fight against child-sex abuse after the Washington meeting approved guidelines designed to push companies such as Google, Facebook and Twitter to shut down “Dark Web” sites on their platforms.

The measures are part of a drive to compel the companies to hand over to the Five Eyes agencies information about how to open up the encryption technologies that millions of people employ to protect their privacy from government and

corporate monitoring and interference.

Both Barr and Dutton targeted encryption. Barr said “predators” communicated using “virtually unbreakable encryption.” Dutton echoed him, saying encryption “allows offenders to diversify their methods and evade law enforcement.”

The actual concern of these governments is not “child sex predators,” whose activities are closely monitored by international police agencies, which already have vast interception powers. The overriding fear in ruling circles is that working people worldwide use encrypted messages to discuss and organise free of government eaves-dropping, amid mounting social unrest and political disaffection.

Last Thursday, a day before the Five Eyes announcement, US congressional leaders released a bipartisan bill that threatens to strip the liability protections of internet companies if they do not help block the use of encryption and other privacy safeguards on social media platforms.

Currently, section 230 of the US Communications Decency Act can shield sites from lawsuits over user content. The proposed Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT) would force companies to “earn” their liability protection by complying with anti-encryption measures.

In Australia, equally anxious to block access to encryption services, Dutton has been engaged in a public attack on Facebook since it announced plans to roll out end-to-end encryption from WhatsApp to its other messaging services, Facebook Messenger and Instagram.

The top-level Five Eyes gathering at the White House coincided with the introduction of a bill to the Australian parliament that would clear the way for a reciprocal agreement under the US Clarifying the Lawful Overseas Use of Data Act (the CLOUD Act).

The Trump administration introduced the CLOUD Act in 2018 to force US-based cloud and tech companies to hand over data held offshore. This power is now to be extended to Australia and other close partners.

In a media release, Dutton said the Telecommunications

Legislation Amendment (International Production Orders) Bill was an “essential precondition” for agreements with the US and other countries to replace “outdated, cumbersome processes” for exchanges of electronic information.

Dutton referred to combatting terrorism and paedophilia, yet section 1 of the Bill allows for much wider exchanges. It refers to investigations of “serious offences.” This could cover a vast field, including leaks of government documents and other offences under Australia’s draconian “foreign interference” legislation.

Section 1 also permits the swapping of information connected to “the carrying out by the Organisation of its functions.” This refers to the country’s primary political spy force, the Australian Security Intelligence Organisation (ASIO). In other words, the Bill covers ASIO’s extensive operations, which are, above all, focused on “subversive” activity deemed a threat to the political establishment and capitalist order.

The Bill further allows interception of the communications of a person who is not even under investigation if authorities assert “reasonable grounds” that the suspected “offender” uses that other person’s communications services.

The legislation would compel Australian service providers to hand over data to US authorities if presented with an “international production order.” Hand-picked members of a vetted tribunal, the Security Division of the Administrative Appeals Tribunal, could issue such orders.

The orders could be for (1) interception, to authorise wiretaps of video and voice calls, (2) stored communications from a messaging application or (3) telecommunications “metadata,” including customers’ names, contact details and account information.

The Bill comes just days after ASIO’s head Mike Burgess admitted, in a “threat assessment” speech, that the agency had accessed encrypted data within 10 days of the anti-democratic Assistance and Access Act coming into effect with the Labor Party’s support.

That Act allows intelligence and police agencies to issue “technical assistance notices” or “capability notices” to compel cooperation from technology companies in building weaknesses into products to make them open to hacking or encryption-cracking.

Encrypted data from these operations would be available to the US under the CLOUD Act exchange plan.

In his speech, Burgess alluded to the danger of large-scale violent attacks by right-wing extremists, like the ones seen in Germany and New Zealand. Dutton, however, immediately insisted that “left-wing extremism” posed an equal threat.

The Bill was tabled just after Dutton and Prime Minister Scott Morrison revived a propaganda campaign to justify

plans to formally allow the Australian Signals Directorate (ASD), the electronic eavesdropping and cyber warfare agency, to spy on people inside Australia. The ASD is a key component of the Five Eyes network.

Digital Rights Watch chairperson Lizzie O’Shea told the *Guardian* the latest Bill “largely solidifies in legislation the existing practical cooperation that occurs informally with Australia’s Five Eyes partners.”

O’Shea commented: “Our concern is every time legislation permits increased surveillance capabilities, that becomes the lowest common denominator and our allies can access that same information using powers in Australia to do so.”

A police-state framework is being created, with the complicity and assistance of the internet companies. According to a Facebook transparency report, Australian authorities made 931 requests for user data between January and June 2019, and the company complied with three-quarters of the requests.

This is occurring under conditions of both rising domestic political discontent and sharpening US conflicts with China.

On every front, from encryption-cracking to increased US access to military bases in northern Australia, the Coalition government is placing the country on the frontline of a potentially catastrophic US war against China. This is accompanied by a barrage of anti-China propaganda.

The government is doing so with the support of the opposition Labor Party, which is equally committed to the US military alliance and has backed every move over the past two decades to strengthen the powers of the military and intelligence apparatus.



To contact the WSWS and the
Socialist Equality Party visit:

wsws.org/contact