Spy and police chiefs demand passage of Australian encryption access law

Mike Head
29 October 2018

Facing mounting public opposition, Australia's intelligence and police chiefs are demanding that parliament pass a bill that would set a global precedent for the compulsory cracking open of encryption and other privacy devices.

In effect, the heads of the spy and security apparatus spoke on behalf of the US-led "Five Eyes" worldwide network, which conducts mass monitoring of the world's population, as well as secret bugging operations against targeted governments.

A summit of the Five Eyes countries, held in Australia on August 28–29, called for laws to enable access to encrypted emails, text messages and voice communications. Representing the US, Canada, Britain, Australia and New Zealand, they declared it was necessary to force open "end-to-end encryption" tools.

Without providing any evidence, Australian Security Intelligence Organisation (ASIO) chief Duncan Lewis told a parliamentary committee hearing on October 19 that suspected terrorists were using encrypted messages to plan potential attacks.

"I can confidently say there are suspected terrorists in Australia using encrypted communications and due to that encryption it is impossible for us at this time to intercept and read their communications, despite our existing range of lawful and legal access authorities," Lewis said.

Australian Federal Police (AFP) Commissioner Andrew Colvin made similar unsubstantiated assertions, trying to link the proposed assault on all on-line communications to the endless "war on terrorism."

In other words, despite the introduction of barrages of legislation since 2001 authorising electronic surveillance, computer hacking, detention and interrogation without trial and other measures overturning fundamental civil and democratic rights, the political spy apparatus insists it must have even greater powers.

Lewis himself noted that since 2014, "at about the time I became the Director-General of Security, we've seen 12 tranches of national security legislation pass through the parliament."

The ASIO chief also alluded to the pressure coming from Washington and other "allies" to push the anti-encryption measures through. He told the committee, "it's not only a concern unique here, to Australia, but it's one faced around the globe, as our international allies and partners would attest."

Lewis said ASIO had neither the desire nor the capacity to intercept or collect the communications of Australians en masse. In reality, the Australian agencies work with their Five Eyes partners to monitor the communications of millions of people, as exposed by former US National Security Agency (NSA) whistleblower Edward Snowden and WikiLeaks, founded by Julian Assange.

In the lead-up to the committee hearing, Home Affairs Minister Peter Dutton insisted that the bill's passage was urgent. Dutton, who attended the Five Eyes summit and heads a super-ministry in charge of all the spy and police agencies, said: "Given we are talking about nine out of 10 national security investigations now being impeded because of the use of encryption, we need to deal with it."

The actual concern of the capitalist class and its security apparatuses is not handfuls of terrorists but growing working class hostility to widening social inequality, worsening working and living conditions, the evisceration of civil and democratic rights and the mounting danger of another world war provoked by the US.

At the hearing, a Home Affairs Department official revealed that it had received 15,990 submissions, an indication of popular opposition, but the department contemptuously dismissed nearly all of them—15,130—as "standard campaign responses." Of the 743 "unique individual responses classified as appropriate for consideration," only 55 were treated as "substantive submissions."

Not one member of the bipartisan parliamentary joint committee on intelligence and security questioned the declarations of the ASIO and AFP chiefs. All the MPs, both Liberal-National and Labor, declared their agreement with the need to protect "security" and suggested changes to the bill to enhance the operations of the spy and police agencies, while appearing to address the widespread alarm.

The far-reaching scope of the bill was underscored when Australian Signals Directorate (ASD) director-general Mike Burgess was asked to outline the communications platforms that would be covered. The examples he gave included: "Your banking application; your web browser; your text; your music application on a phone; Signal, which is a messaging app that encrypts data; WhatsApp."

The ASD, Australia's equivalent of the US NSA, conducts electronic surveillance, including bugging and phone tapping, throughout the Indo-Pacific region.

Under the Telecommunications (Assistance and Access) Bill 2018, telcos, Internet companies and device manufacturers, as well as website and individual social media hosts, would be compelled to remove all barriers to government agencies accessing private data.

Companies would face fines of up to $10 million for each instance of "non-compliance" with "technical assistance notices" or "technical capability notices." Individuals could be fined up to $50,000.

The ASIO and AFP chiefs repeated the government's claims that the legislation would not require tech companies to provide "backdoor" entry to encryption systems. But any "approved agency" could force an individual or a service provider to hand over a password or the tools to decrypt messages.

Other witnesses at the hearing outlined insidious aspects of the 176-page bill. Several pointed out that it only mentions "encryption" once. Instead, it uses the wider term "electronic protection" to cover all devices and applications designed to ensure privacy.

Arthur Moses, the president-elect of the Law Council, representing the legal profession, said: "The bill as presently drafted would authorise the exercise of intrusive covert powers with the potential to significantly limit an individual's right to privacy."

Moses said compliance notices could amount to a new form of detention without trial. "If a person is required to attend a place to provide information or assistance, this may amount to detention of that person, particularly as they may be arrested on suspicion of an offence if they attempt to leave."

The Law Council also warned that the bill would allow authorities to side-step warrants previously needed to access private information.

Despite raising objections to aspects of the bill—particularly the threat of criminal sanctions for non-compliance—executives from the major telecommunications companies stressed their willingness to keep voluntarily collaborating with the authorities.

Ramah Sakul, a representative of Telstra, Australia's largest telecommunications company, told the hearing: "We believe a collaborative and cooperative approach is more likely to result in efficient and timely outcomes in the provision of assistance and capability development."

Andrew Sheridan from Optus said his company had "developed a long history of cooperation with law enforcement and national security agencies," including "data retention."

Representing "The Software Alliance" of transnational internet corporations, such as Google, Facebook and Amazon, Darryn Lim said his organisation "encourages close collaboration between the government, Australian law enforcement and the technology community to improve processes and methodologies enabling law enforcement access to digital evidence in a timely manner."

Lim outlined a six-point plan to modify the bill to enhance this relationship.

As the WSWS has documented in detail, the global giants are increasingly working in partnership with governments to implement anti-democratic restrictions on internet access. This features, in particular, using algorithms to limit or block access to socialist, anti-war and other critical websites.

The WSWS has called for the formation of an International Coalition of Socialist, Anti-War and Progressive Websites to fight this attack on freedom of speech and basic democratic rights.