Australian government to impose encryption-cracking bill with Labor's support

Mike Head
6 December 2018

After days of intensive backroom collaboration, the opposition Labor Party today sought to assist the crisis-wracked Liberal-National Coalition government to push through encryption-cracking and computer-accessing laws during the final hours of this year's last parliamentary session.

Labor's support for the bill, with only token amendments, will hand extraordinary powers to the spy and police forces, setting a global precedent that has been demanded by the US intelligence and military establishment.

The Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 will allow an array of state and federal agencies, including the Australian Border Force, to access encrypted and other privacy-protected communications, including WhatsApp or iMessage conversations.

They also will be able to secretly hack into and manipulate people's computers—a power currently reserved for the Australian Security Intelligence Organisation (ASIO), the domestic political spy agency.

This is a fundamental attack on basic democratic rights, including privacy, free speech and the right to organise, especially against the corporate and political establishment. It is part of an escalating barrage of measures designed to suppress dissent and social unrest.

By helping Prime Minister Scott Morrison's government fast-track the slightly amended bill—allowing almost no public debate in parliament—the Labor Party sent two clear signals to the ruling capitalist class.

The first is that the Labor leaders will try to prop up this government until it calls a federal election, either in March or May, in an effort to stabilise the increasingly loathed and discredited parliamentary order. Labor does not want the government brought down in a way that could open the door for a wider working-class movement against the entire political establishment.

The second message is the Labor Party is ready to form a repressive government under conditions of emerging economic slump, mounting popular discontent and a US-led drive for war against China.

In the final two-week parliamentary session of the year, Labor also joined hands with the government to bring forward four other bills with police-state provisions. These will allow the government to call out the military to put down domestic unrest; fast-track a new "foreign interference" register; strip citizenship from anyone convicted of even a minor terrorism-related offence; and permit Australian Secret Intelligence Service (ASIS) operatives—Australia's foreign spies—to kill people to protect their clandestine missions.

The government proclaimed a victory after Labor dropped a request for them to agree to initially push through a temporary version of the encryption and computer hacking laws, supposedly limiting their use to federal agencies targeting terrorists and paedophiles.

Attorney-General Christian Porter described the deal as a "massive win." He said Labor had "moved very substantially" from its so-called compromise offer, which would have delayed part of the bill until the outcome of a parliamentary intelligence and security committee review.

Labor's legal affairs spokesman Mark Dreyfus said the government had "trashed" the intelligence committee process but welcomed the retention of the bipartisan unity that has imposed wave after wave of new measures to boost the powers of the state apparatus.

"Labor has spent five years responsibly improving national security legislation to make Australians safer, and we have done the same thing today," Dreyfus said. In fact, Labor has worked hand-in-glove with the Coalition since 2001, both in opposition and in office, to impose one package of draconian laws after another.

These included the metadata retention legislation of 2015, which already gave the police and intelligence agencies the power to access everyone's online data, going back up to two years. There has been bipartisan agreement on expanding such powers since 1979, when ASIO first obtained the legal authority to tap into telecommunications and computers.

"They already have powers to hack end points, where information is not encrypted," Monique Mann, a Queensland University of Technology law and technology researcher, told the Australian Broadcasting Corporation (ABC).

Labor's request for a narrower initial regime was not driven by any concern for democratic rights. Instead, it voiced the interests of the internet and social media conglomerates, which said handing the powers to a broad range of government agencies would increase the danger of encryption-cracking tools falling into unwanted hands. The companies were concerned that this could threaten the highly-profitable use of encryption by themselves and other giant corporations, including banks and retail operators.

Under the deal struck between Labor and the Coalition, the anti-encryption powers will be available to investigate "serious crimes"—defined as all terrorism and child sex offences, and other offences punishable by imprisonment for three years or more. This covers a wide range of offences, including the new crimes of being involved in "foreign interference" or failing to register under the "foreign influence transparency scheme."

As a supposed safeguard against abuse, law enforcement and spy agencies will not be able to issue "technical capability notices," which can force companies to install software or modify their systems to enable encryption-cracking, unless both the attorney-general and communications minister approve. Placing this process in the hands of two senior cabinet ministers can hardly be regarded as a protection. Instead, it facilitates the use of the new powers for political purposes.

The agreed bill contains a definition of "systemic weakness"—which companies cannot be asked to create—and stipulates that disputes about what constitutes such an impermissible "back door" will be determined by a former judge and a person with technical expertise. Giving such figures scrutiny over these disputes may assuage the telco giants but it will not protect ordinary people.

Where companies are compelled to comply with encryption-breaching notices, or agree to do so voluntarily, these processes will remain hidden from retail users. It will be illegal for companies to inform their customers that they have handed information over to the authorities.

According to an ABC report, technology giants like Apple and Google already voluntarily assist the authorities. During July-December 2017, for instance, Australian police made 120 requests for Apple account details, which could include someone's iCloud content. Apple provided data in 64 percent of these cases.

Business organisations generally backed the Labor-Coalition deal for shielding their interests. Ai Group chief executive Innes Wilox said the changes "appear to go some way to addressing a number of the concerns … Protecting the security of communications and information between businesses and their customers is of fundamental importance."

The Australian bill is regarded as a test case for similar legislation in the US and other places, and will facilitate surveillance across the global US-led "Five Eyes" spy network. Capitalist governments, in collaboration with social media companies like Google and Facebook, also are implementing restrictions on internet access, particularly designed to limit or block access to the *World Socialist Web Site* and other left wing, anti-war and progressive websites.

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