Australian encryption bill becomes a global test case for surveillance

Mike Head
10 October 2018

Acting as part of the US-led "Five Eyes" intelligence network, the Australian government is seeking to push through parliament an encryption-cracking bill that would set an international precedent for far-reaching internet surveillance.

Despite widespread opposition, reflected in more than 14,000 submissions by concerned individuals and companies, the government tabled the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 in parliament last month with only minor amendments.

Prime Minister Scott Morrison's Liberal-National government seems intent on getting the bill into law before the end of the year. It has scheduled only a one-day public hearing by the parliamentary intelligence and security committee. The members of that committee, including those from the Labor Party, have close connections with the US and allied spy agencies.

Telcos, internet companies, device manufacturers and website and social media hosts face fines of up to $10 million for each instance of "non-compliance." They would be compelled to facilitate the cracking of encryption codes and remove other barriers to government agencies accessing private data. Individuals can be fined up to $50,000.

The intelligence and police forces would be able to issue technical assistance requests (TARs), technical assistance notices (TANs) and technical capability notices (TCNs). These would compel any company or individual to build capabilities or functionalities to provide any information required by the agencies.

These powers would potentially affect any website or Facebook page. According to government ministers, they would apply to encrypted messaging services such as WhatsApp, as well as "any entity operating a website."

Despite repeated government denials that it would force service providers to build back doors to break passwords and undermine encryption, the legislation states otherwise. While section 317ZG of the draft bill says communications providers "must not be required to implement or build a systemic weakness or systemic vulnerability," section 317E sets out a long list of "acts or things" that providers can be compelled to do.

These include "(a) removing one or more forms of electronic protection ... (c) installing, maintaining, testing or using software or equipment … (h) modifying, or facilitating the modification of, any of the characteristics of a service provided by the designated communications provider."

The vague language appears to permit the type of demand that the US Federal Bureau of Investigation (FBI) made in 2016 when it sought a court order to compel Apple to help unlock an iPhone belonging to a suspect in a shooting.

Government agencies would only have to allege that a TAN or TCN is "reasonable and proportionate" and "practicable and feasible." These are undefined and sweeping terms. There would be no review process before notices are issued and the bill is silent on how a recipient could challenge a notice as unlawful.

Moreover, the bill's strict non-disclosure provisions mean that "affected persons"—that is, internet users—would never know a notice has been issued. Section 317ZF provides that individuals who disclose information regarding a notice may be subject to five years' imprisonment.

The legislation would also make it easier for the political surveillance agencies, such as the Australian Security Intelligence Organisation (ASIO), to search computers covertly. Current laws permit them to monitor communications and data during transmissions. The changes would allow them to access and copy stored data, building on the "metadata access" laws pushed through, with the Labor Party's support, in 2015.

This is part of a wider build-up of police-state powers in the hands of the capitalist state apparatus. Repeated barrages of legislation have been imposed by one government after the next, Liberal-National and Labor alike. Supposedly aimed at combatting terrorism, these powers are designed to monitor and crack down on political dissent.

A number of civil rights organisations, such as Digital Rights Watch, the Human Rights Law Centre, Amnesty International and Access Now, this month joined industry bodies, including those representing transnational internet companies like Google, Facebook and Apple, in an "Alliance for a Safe and Secure Internet" to object to features of the bill.

Most of these groups signed a submission warning that the bill's definition of "designated communications providers" could affect hundreds of thousands, if not millions, of individuals in Australia and around the world.

As the submission documented, the bill's Explanatory Document states that "designated communications provider" would extend to anyone who "provides an electronic service that has one or more end-users in Australia." This could include banks, media companies, insurers and universities, as well as news sites and those of political parties.

Likewise, "electronic services" are broadly defined. They "may include websites and chat fora, secure messaging applications, hosting services including cloud and web hosting, peer-to-peer sharing platforms and email distribution lists, and others." These powers would apply globally, since the notices could be served outside Australia.

Aware of popular hostility to internet censorship, the "Safe and Secure Internet" alliance is posturing as a defender of civil liberties. A spokesman, Communications Alliance chief executive John Stanton, said: "The scope of this legislation sets a disturbing first-world benchmark and poses real threats to the cybersecurity and privacy rights of all Australians."

The alliance's perspective, however, is to seek certain modifications of the bill. It wants to enhance the already extensive collaboration between governments, the political spy agencies and the social media conglomerates to control or manipulate the internet in order to restrict access to left-wing and progressive web sites, and especially the *World Socialist Web Site* (WSWS).

"Instead of trying to ram this legislation through the committee process and the parliament, the government needs to sit down with stakeholders, engage on the details and collectively come up with workable, reasonable proposals that meet the objective of helping enforcement agencies be more effective in the digital age," Stanton said.

Government officials told the *Australian Financial Review* the industry had generally been co-operative with requests for information, but sought a legal framework because of concerns that customers would hold them legally liable for disclosing information to agencies.

A meeting of cabinet members from the so-called Five Eyes global spying network, held in Australia on August 28–29, demanded access to encrypted emails, text messages and voice communications through legislation. Representing the US, Canada, Britain, Australia and New Zealand, they issued a statement on combatting "ubiquitous encryption," declaring the necessity to crack open "end-to-end encryption" tools.

Given the importance of encryption for online retail, banking and other corporate and financial purposes, the statement denied any "intention to weaken encryption mechanisms." Nonetheless, the five governments "agreed to the urgent need for law enforcement to gain targeted access to data," subject to further "discussion with industry."

As the WSWS has proven, these governments and their European counterparts are increasingly working in partnership with social media companies to implement anti-democratic restrictions on internet access. This went to a new level in April 2017, when Google announced new algorithms, aimed at limiting or blocking access to socialist, anti-war and other critical websites. Facebook and Twitter have since adopted similar measures.

The WSWS has taken the lead in exposing this conspiracy to censor the internet. It has called for the formation of an International Coalition of Socialist, Anti-War and Progressive Websites to fight back against this attack on freedom of speech and basic democratic rights.