Home Affairs encryption bill: A political tool made in Britain

By Elisa Barwick

Australia's Home Affairs Department, created to streamline coordination of intelligence with the British Secret Service-led Five Eyes spying alliance (USA, UK, Canada, Australian, New Zealand), has produced legislation to allow Australia's intelligence and law enforcement agencies unprecedented access to the private data of citizens.

A draft of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, first announced in July 2017, was released publicly on 14 August and is open for consultation only until 10 September (assistancebill.consultation@homeaffairs.gov.au). Developed by Home Affairs in conjunction with agencies such as the Australian Security Intelligence Organisation (ASIO), the bill takes aim at the encryption of web transactions and communications, based on the fact that criminal networks also depend upon such protections to transact their business without being caught.

According to the Home Affairs Department, the legislation would force domestic and offshore providers supplying internet-based communications services and devices to assist Australian law enforcement in its pursuits; would create new computer access warrants enabling law enforcement to *covertly* access devices and collect evidence; and would strengthen existing search and seizure warrants for *overt* access to data.

California-based digital civil liberties group, Electronic Frontier Foundation (EFF), says the legislation "unashamedly lifts its terminology and intent from the British law" passed in November 2016, the *Investigatory Powers Act* (IPA, a.k.a. the Snoopers' Charter), sharpening its powers even further. It would allow the government to demand that tech companies re-engineer or substitute apps, services or programs to enable surveillance to be conducted, to hack into computers, or remotely access private data, supposedly to protect national security. Telcos, Internet Service Providers (ISPs), software developers, websites, chat groups, messaging and other apps, email distribution companies, hosting services, etc., would have to comply. The orders and any consequences for consumers would remain secret. The penalty for disclosing information is five years' imprisonment; for not complying with an assistance order, 5-10 years!

Authorities could target individual app or software developers, whether a hobbyist or employee of a multinational company. The wording of the equivalent UK legislation allows authorities to seek out particular employees of a company to conduct a task *without informing his or her employer*. It is even possible to force a coffee shop chain providing free WiFi to deploy malware on its customers, on behalf of the British secret service, according to EFF's Danny O'Brien.

The Australian bill does not allow electronic protections currently afforded to consumers to be weakened, but this and other concessions are "tiny exceptions in a sea of permissions, and easily circumvented", noted EFF. The language is broad enough to allow for far-reaching breaches of privacy, and there is no real oversight other than the Attorney General. For instance, the phrase "any other thing reasonably incidental to any of the above" appears 11 times in the legislation in reference to what specific actions are authorised by various warrants.

A global campaign

In the name of threats to national security from terrorists and hostile foreign states, the UK is working to bring domestic laws around the world into line with the types of illegal spying activities exposed by US National Security Agency (NSA) whistleblower Edward Snowden in 2013.

These claimed threats are a ruse. Terrorism is a very real threat, but it has been actively cultivated by UK and US governments and their proxies to justify regime change against "rogue" states (*Stop MI5/MI6-run Terrorism!*, CEC, June 2017). As for foreign state threats, accusations against Russia and China are often hyped and even baseless, such as when China was falsely accused of hacking Australia's census. And somehow spying on all of us is supposed to allay these threats, despite the fact that experts such as William Binney, a former technical director at the NSA who testified against the IPA in the British Parliament, have demonstrated that mass collection of data swamps the real intelligence capabilities required to stop terrorist threats. ("London/Manchester terrorism report a whitewash", *AAS* 13 Dec. 2017.)

Britain's Home Secretary Sajid Javid pushed the foreign interference barrow at the Five Eyes ministerial meeting on Australia's Gold Coast on 28-29 August, following unproven claims that Russia was behind the March poisoning of Sergei and Yulia Skripal in Salisbury, England. Australia has been a leading nation in the Five Eyes' push for a new standard of state-secrecy to prevent foreign interference—on 28 June the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* was passed, smothering freedom of speech, association and political communication.

The UK's IPA legislation was a precursor to this, introduced by Theresa May in 2015 when she was Home Secretary. When it passed in late 2016, she immediately began talking about the necessity for equivalent powers globally. In early 2016, Britain had already begun negotiating a reciprocal agreement with its US counterparts, whereby the UK could quickly access customer data from US social media or email servers, and vice versa. At the moment this occurs only by formal application to the foreign counterpart's domestic justice system, a very slow process. End-to-end encryption used by many internet services adds to the difficulty, as data is accessible only at its point of origin and final destination, with no access provided to the mediating party.

This is the context for the encryption bill; the same intent was evident in the Official Communiqué of the Five Eyes Ministerial meeting, which had been billed by Australia's Home Affairs Secretary Michael Pezzullo to include "trailblazing" initiatives ("Five Eyes plan global police state", *AAS* 22 Aug.) The spying forum was refocused, the Communiqué said, around collaboration on matters including counter-terrorism, cyber security, foreign interference and border management. The five countries promised they would gang up to deal with any "severe foreign interference incident". On encryption, the statement declared that while "The five countries have no interest or intention to weaken encryption mechanisms", there is an "urgent need for law enforcement to gain targeted access to [encrypted] data".

With a new global economic crisis shaking up the political spectrum, the possibility has never been greater that rebellious voters can force policy changes that will take power away from the City of London and Wall Street Establishment. It is clear that the myriad of new police-state powers are intended to provide the means to suppress democratic revolts that threaten the Establishment.