GlobalResearch
Center for Research on Globalization

The Security Derangement Complex: Technology Companies and Australia's Anti-Encryption Law

By Dr. Binoy Kampmark
Global Research, December 07, 2018
Region: Oceania
Theme: Intelligence, Law and Justice

Australia is being seen as a test case. How does a liberal democracy affirm the destruction of private, encrypted communications? In 2015, China demonstrated what could be done to technology companies, equipping other states with an inspiration: encryption keys, when required, could be surrendered to the authorities.

It is worth remembering the feeble justification then, as now. As Li Shouwei, deputy head of the Chinese parliament's criminal law division explained to the press at the time, "This rule accords with the actual work need of fighting terrorism and is basically the same as what other major countries in the world do". Birds of a feather, indeed.

An Weixing, head of the Public Security Ministry's Counter-Terrorism division, furnishes us with the striking example of a generic state official who sees malefactors coming out of the woodwork of the nation. "Terrorism," he sombrely stated, reflecting on Islamic separatists from East Turkestan, "is the public enemy of mankind, and the Chinese government will oppose all forms of terrorism." Given that such elastic definitions are in the eye of the paranoid beholder, the scope for indefinite spread is ever present.

The Australian Prime Minister, Scott Morrison, must be consulting the same oracles as those earning their keep in the PRC. The first rule of modern governance: frighten the public in order to protect them. Look behind deceptive facades to find the devil lurking in his trench coat. Morrison's rationale is childishly simple: the security derangement complex must, at all times, win over. The world is a dark place, a jungle rife with, as Morrisons insists upon with an advertiser's amorality, paedophile rings, terrorist cells, and naysayers.

One of his solutions? The Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, otherwise known by its more accurate title of the Anti-Encryption Bill. This poorly conceived and insufferably vague Bill, soon to escape its chrysalis to become law, shows the government playbook in action: tamper with society's sanity; draft a ponderous bit of text; and treat, importantly, the voter as a creature mushrooming in self-loathing insecurity in the dark.

The Bill, in dreary but dangerous terms, establishes "voluntary and mandatory industry assistance to law enforcement and intelligence agencies in relation to encryption technologies via the issuing of technical assistance requests, technical assistance notices and technical capability notices". Technology companies are to become the bullied handmaidens, or "assistants", of the Australian police state.

The Pentecostal Prime Minister has been able to count on supporters who see privacy as dispensable and security needs as unimpeachable. Those who get giddy from security

derangement syndrome don the academic gown of scorn, lecturing privacy advocates as ignorant idealists in a terrible world. "I know it is a sensitive issue," claims Rodger Shananan of the Lowy Institute for International Policy, "but the people arguing privacy just don't have a handle on how widespread it's used by the bad people." The problem with such ill-considered dross is that such technology is also used by "good" or "indifferent" people.

Precisely in being universal, inserting such anti-encryption backdoors insists on a mutual presumption of guilt, that no one can, or should be trusted. It is in such environments that well versed cyber criminals thrive, sniffing out vulnerabilities and exploiting them. Computing security academic Ahmed Ibrahim states the point unreservedly. "If we leave an intentional backdoor they will find it. Once it is discovered it is usually not easy to fix."

The extent of such government invasiveness was such as to trouble certain traditional conservative voices. Alan Jones, who rules from the shock jock roost of radio station 2GB, asked Morrison about whether this obsession with back door access to communications might be going too far. Quoting Angelo M. Codevilla of Boston University, a veteran critic of government incursions into private, encrypted communications, Jones suggested that the anti-encryption bill "allows police and intelligence agencies access to everyone's messages, demanding that we believe that any amongst us is as likely or not to be a terrorist." Morrison, unmoved, mounted the high horse of necessity. Like Shanahan, he was only interested in the "bad" people.

To that end, public consultation has been kept to a minimum. In the words of human rights lawyer, Lizzie O'Shea, it was "a terrible truncation of the process", one evidently designed to make Australia a shining light for others within the Five Eyes Alliance to follow. "Once you've built the tools, it becomes very hard to argue that you can't hand them over to the US government, the UK – it becomes something they can all use."

There had been some hope that the opposition parties would stymy the process and postpone consideration of the bill till next year. It could thereby be tied up, bound and sunk by various amendments. But in the last, sagging sessions of Australia's parliament, a compliant opposition party was keen to remain in the elector's good books ahead of Christmas. Bill Shorten's Labor Party took of the root of unreason, calculating that saying yes to the contents of the bill might also secure the transfer of desperate and mentally ailing refugees on Nauru and Manus Island to the Australian mainland.

Instead, in what became a farcical bungle of miscalculating indulgence, the government got what it wanted. The medical transfer bill on Nauru and Manus Island failed to pass in the lower house after a filibuster in the Senate by the Coalition and Senators Cory Bernardi and Pauline Hanson. The Anti-Encryption Bill, having made is way to the lower house, did.

Shorten's deputy, Tanya Plibersek, was keen to lay the ground for Thursday's capitulation to the government earlier in the week. A range of "protections" had been inserted into the legislation at the behest of the Labor Party. (Such brimming pride!) The Attorney-General Christian Porter was praised – unbelievably – for having accepted their sagacious suggestions. The point was elementary: Labor, not wanting to be seen as weak on law enforcement, had to be seen as accommodating.

Porter found himself crowing. "This ensures that our national security and law enforcement

agencies have the modern tools they need, the appropriate authority and oversight, to access the encrypted conversations of those who seek to do us harm."

International authorities versed in the area are looking at the Australian example with jaw dropping concern. EU officials will find the measure repugnant on various levels, given the General Data Protection Regulation (GDPR) laws in place. Australian technology companies are set to be designated appropriate pariahs, as are other technology companies willing to conduct transactions in Australia. All consumers are being treated as potential criminals, an attitude that does not sit well with entities attempting to make a buck or two.

SwiftOnSecurity, an often canonical source on cyber security matters, is baffled. "Over in Australia they're shooting themselves in the face with a shockingly technical nonsensical encryption backdoor law." Not only does the law fail to serve any useful protections; it "poison-pills their entire domestic tech industry, breaks imports."

Li's point, again something which the Australian government insists upon, was that the Chinese law did not constitute a "backdoor" through encryption protections. Every state official merely wanted to get those "bad people" while sparing the "good". The Tor Project is far more enlightening: "There are no safe backdoors." An open declaration on the abolition of privacy in Australia has been made; a wonderfully noxious Christmas present for the Australian electorate.

*

Note to readers: please click the share buttons above. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

Dr. Binoy Kampmark was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. He is a frequent contributor to Global Research and Asia-Pacific Research. Email: bkampmark@gmail.com

Featured image is from Softpedia News
