Australian Government Missed the Point with New Encryption Bill

15 May 2019

By Associate Professor Christophe Doche and Dr John Selby

The government's Assistance and Access Act will have little effect against cybercriminals and terrorists, but it threatens Australian tech companies and undermines individual rights.

The Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, also dubbed "the encryption bill" was passed by parliament in December 2018. It requires technology companies and telecommunications providers to give reasonable assistance to law enforcement agencies to access communication content and data. For a very complete and detailed analysis of the bill and its implications, we refer to this excellent article by Matt Shearing.

In a nutshell, this new Act is an attempt to address challenges faced by law enforcement agencies when dealing with criminal cases where data that could provide evidence cannot be accessed because it is encrypted. Although its goals are laudable, we argue that, in practice, the Assistance and Access Act will have little effect against cybercriminals and terrorists but represents serious threats to individual rights and the competitiveness of Australian tech companies.

Inadequacy of the new Act

Former Australian Attorney-General George Brandis said in 2017: "At one point or more of that process, access to the encrypted communication is essential for intelligence and law enforcement" and added that a new law needs to be "sufficiently strong to require companies, if need be, to assist in response to a warrant to assist law enforcement or intelligence to decrypt a communication." Such assistance may come in the form of alterations/updates to hardware, networks or software that replace secure encryption systems with modified (weakened) encryption systems.

Whilst the first part of Brandis' statement may be true, the second part shows a deep misunderstanding of the technology landscape, in particular how encryption can be created as it is not exclusively available off-the-shelf through technology companies and telecommunications service providers. Implementing a backdoor in encrypted services offered by a company, in other words introducing a systematic weakness in new or existing encryption tools to allow a law enforcement agency to decrypt any message, is of little use against determined criminals or terrorists. Beyond the questionable idea of weakening an encryption system (since the vulnerability can be exploited by any one who becomes aware of the backdoor, be they police or criminals), what decision makers do not seem to realise or acknowledge is that the cryptographic genie is out of the bottle, and there is no way it is getting back in.

For instance, a German company recently released the first decentralised encrypted messenger service. Such tools have no central point of attack, no option to switch them off, and of course no opportunity to introduce a backdoor. That is not all. Modern cryptography is very well understood – encryption tools, precise implementation guidelines and design principles are readily accessible everywhere. This knowledge is being taught in cryptography courses in universities around the country. All this information provides a range of solutions for users who feel they can no longer rely upon technology companies or telecommunications service providers. If a person does not trust a particular vendor or service provider (because they could be ordered by an Australian government agency to implement a backdoor) it is actually relatively simple to implement your very own encryption software. This is exactly what the cyber security expert who worked on the movie *Snowden* as technical advisor did. He provided a custom-made encrypted communication platform for the entire film crew because there were concerns that different people wanted to access their work.

We have to accept that it is relatively easy for a range of actors who do not depend upon technology companies or telecommunications service providers, whether motivated by noble or evil purposes, to access or create efficient and highly secure encryption systems. And they are unbreakable, no matter how hard anybody tries – including Australia's government agencies.

Therefore, this new law will only encourage criminals to stay away from mainstream companies providing encrypted services and force them to adopt more stealthy and custom communication systems. But that is not the only effect it will have.

Risks to industry and privacy

Due to the perceived risk of a "foreign" government's ability to interfere with the security and trustworthiness of its devices, the Australian government prohibited Huawei from tendering to supply hardware to build Australia's 5G network. The Assistance and Access Act effectively co-opts Australia's technology private sector to interfere with the security and trustworthiness of our technology as unwilling extensions of Australia's intelligence and law enforcement agencies. Due to the Act, foreign governments and foreign businesses will likely take a similar approach when Australian businesses tender to export their technology and cybersecurity hardware, software and services to foreign customers. In the context of widely publicised examples of Australia actively spying on its neighbours (as revealed in the Edward Snowden leaks and the bugging of East Timor's cabinet office), why would a foreign government or foreign business take the risk of including within their IT systems goods or services provided by Australian businesses that may contain secret backdoors ordered by Australian (or other Five Eyes) government agencies? In the face of such a threat to their business models and export plans, it is unsurprising to see resistance to the Assistance and Access Act from many of Australia's leading Internet companies, Atlassian being a prime example.

The Assistance and Access Act risks making Australia's technology companies a playground for foreign spies. Whilst it is relatively easy for an Australian business owner or employee to drive to their local police station to check whether an instruction given by a police officer is official, it is not so easy to verify that an instruction given by an "intelligence agent" is official (unlike the police, Australia's intelligence agencies don't tend to have an office every few suburbs). Imagine a technology company's employee is approached at home one morning before work by a person claiming to be an Australian government intelligence agency official who waves a piece of paper under the employee's nose and orders them to secretly alter the codebase of their employer's product (and forbids the employee to tell their employer about it under threat of imprisonment). Despite what is written in the Act, how can the employee easily verify that the order has been given by an *Australian* agent and not a foreign agent impersonating an Australian agent? The employee is unlikely to have the funds to hire a lawyer to assist them (particularly if the foreign intelligence agent has selected the employee precisely because they are financially vulnerable) and therefore is quite likely to simply comply with the order without checking its legitimacy.

Unlike the other members of the Five Eyes, Australia lacks constitutional privacy protections through a Bill of Rights at a federal level, which could offer its citizens more readily available means to challenge the validity of the Assistance and Access Act through the courts. Some have claimed that this was precisely why Australia was chosen as the location to pass this Act (so that the other members of the Five Eyes intelligence agencies could bypass their own domestic constitutional limitations by laundering their requests via Australia). Whilst the Australian Competition and Consumer Commission has recently recommended the creation of both statutory and private rights of action for serious invasions of privacy, these could only offer Australians partial remedies (only against law enforcement agencies) as Australia's intelligence agencies are excluded from the jurisdiction of the Privacy Act.

Without amendments to the Assistance and Access Act or its repeal by parliament, it is unclear how it will deter criminals or terrorists. Instead, it will increase risks to Australian businesses and individuals. Creative lawyering and creative coding may be our best hopes to fix these problems.

Associate Professor Christophe Doche is executive director of the Optus Macquarie University Cyber Security Hub, the first initiative of this kind in Australia, linking academics in information security,

business, criminology, intelligence, law and psychology together with cyber security experts from industry. As part of his role, he oversees research, education and thought leadership activities in cyber security.

Dr John Selby is a lawyer, an academic at the Macquarie Business School and an active member of the Optus-Macquarie University Cyber Security Hub who researches on the spill-over effects of new technologies on business and society, including cyber security, privacy and artificial intelligence. He is currently leading an interdisciplinary team investigating identity theft due to mobile phone porting.