Written by Monique Mann, Vice Chancellor's Research Fellow in Regulation of Technology, Queensland University of Technology

The Australian government has released a draft of its long awaited bill to provide law enforcement and security agencies with new powers to respond to the challenges posed by encryption
.

According to the Department of Home Affairs , encryption already impacts 90% of Australian Security Intelligence Organisation's (ASIO) priority cases, and 90% of data intercepted by the Australian Federal Police. The measures aim to counteract estimates that communications among terrorists and organised crime groups are
expected
to be entirely encrypted by 2020.

The Department of Home Affairs and ASIO can already access encrypted data with specialist decryption techniques – or at points where data are not encrypted. But this takes time. The new bill aims to speed up this process, but these broad and ill-defined new powers have significant scope for abuse.

Read more: ***New data access bill shows we need to get serious about privacy with independent oversight of the law***

The Department of Home Affairs argues this new framework will not compel communications providers to build systemic weaknesses or vulnerabilities into their systems. In other words, it is not a backdoor.

But it will require providers to offer up details about technical characteristics of their systems that could help agencies exploit weaknesses that have not been patched. It also includes installing software, and designing and building new systems.

Compelling assistance and access

The draft Assistance and Access Bill introduces three main reforms.

First, it increases the obligations of both domestic and offshore organisations to assist law enforcement and security agencies to access information. Second, it introduces new computer access warrants that enable law enforcement to covertly obtain evidence directly from a device (this occurs at the endpoints when information is not encrypted). Finally, it increases existing powers that law enforcement have to access data through search and seizure warrants.

The bill is modelled on the UK's Investigatory Powers Act , which introduced mandatory decryption obligations. Under the UK Act, the UK government can order telecommunication providers to remove any form of electronic protection that is applied by, or on behalf of, an operator. Whether or not this is technically possible is another question.

Similar to the UK laws, the Australian bill puts the onus on telecommunication providers to give security agencies access to communications. That might mean providing access to information at points where it is not encrypted, but it's not immediately clear what other requirements can or will be imposed.

Read more: ***End-to-end encryption isn't enough security for 'real people'***

For example, the bill allows the Director-General of Security or the chief officer of an interception agency to compel a provider to do an unlimited range of *acts or things*. That could mean anything from removing security measures to deleting messages or collecting extra data. Providers will also be required to conceal any action taken covertly by law enforcement.

Further, the Attorney-General may issue a "technical capability notice" *directed towards ensuring that the provider is capable of giving certain types of help* to ASIO or an interception agency.

This means providers will be required to develop new ways for law enforcement to collect information. As in the UK, it's not clear whether a provider will be able to offer true end-to-end encryption and still be able to comply with the notices. Providers that breach the law risk facing $10 million fines.

Cause for concern

The bill puts few limits or constraints on the assistance that telecommunication providers may be ordered to offer. There are also concerns about transparency. The bill would make it an offence to disclose information about government agency activities without authorisation. Anyone leaking information about data collection by the government – as Edward Snowden did in the US – could go to jail for five years.

There are limited oversight and accountability structures and processes in place. The Director-General of Security, the chief officer of an interception agency and the Attorney-General can issue notices without judicial oversight. This differs from how it works in the UK, where a specific judicial oversight regime was established, in addition to the introduction of an Investigatory Powers Commissioner.

Notices can be issued to enforce domestic laws and assist the enforcement of the criminal laws of foreign countries. They can also be issued in the broader interests of national security, or to protect the public revenue. These are vague and unclear limits on these exceptional powers.

Read more: ***Police want to read encrypted messages, but they already have significant power to access our data***

The range of services providers is also extremely broad. It might include telecommunication companies, internet service providers, email providers, social media platforms and a range of other " over-the-top " services. It also covers those who develop, supply or update software, and manufacture, supply, install or maintain data processing devices.

The enforcement of criminal laws in other countries may mean international requests for data will be funnelled through Australia as the “weakest-link” of our Five Eyes allies. This is because Australia has no enforceable human rights protections at the federal level.

It's not clear how the government would enforce these laws on transnational technology companies. For example, if Facebook was issued a fine under the laws, it could simply withdraw operations or refuse to pay. Also, $10 million is a drop in the ocean for companies such as Facebook whose total revenue last year exceeded US$40 billion.

Australia is a surveillance state

As I have argued elsewhere , the broad powers outlined in the bill are neither necessary nor proportionate. Police already have existing broad powers, which are further strengthened by this bill, such as their ability to covertly hack devices at the endpoints when information is not encrypted.

Australia has limited human rights and privacy protections. This has enabled a constant and steady expansion of the powers and capabilities of the surveillance state. If we want to protect the privacy of our communications we must demand it.

The *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Cth) is still in a draft stage and the Department of Home Affairs invites public comment up until 10th of September 2018. Submit any comments to assistancebill.consultation@homeaffairs.gov.au.

Dr Monique Mann is a Board Member of the Australian Privacy Foundation where she Co-Chairs the Surveillance Committee. She is also on the Advisory Council of Digital Rights Watch Australia. While at the Australian Institute of Criminology, she consulted for the Australian Criminal Intelligence Commission on information systems and cybercrime. The views expressed here are those of the author and do not represent the views of any Commonwealth agency.

Authors: Monique Mann, Vice Chancellor's Research Fellow in Regulation of Technology, Queensland University of Technology

Written by Monique Mann, Vice Chancellor's Research Fellow in Regulation of Technology, Queensland University of Technology

Read more http://theconversation.com/the-devil-is-in-the-detail-of-government-bill-to-enable-access-to-communications-data-96909