From: Peacock, Justin (Housing)
To: Assistance Bill Consultation
Subject: the Assistance & Access bill - comment
Date: Monday, 20 August 2018 11:01:22 AM
Attachments: image001.png

I am writing to you in opposition to the Assistance & Access bill.

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.

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.

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.

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.

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 Australia as a surveillance state.

Regards,

Justin Peacock
Project Officer
Housing Strategy & Development
P: [redacted] | E: [redacted]

[redacted]
Visit Housing SA at: www.sa.gov.au/housing

SA Housing Authority

Government of South Australia