From: Emily Olorin
To: Assistance Bill Consultation
Subject: Submission to consultation on the Assistance and Access Bill 2018
Date: Friday, 7 September 2018 6:01:12 PM

The Bill grants the Director-General of Security, the chief officer of an interception agency and the Attorney-General additional powers to issue new types of orders. These include forcing communications and technology companies to provide information about how networks are built and how information is stored, or to directly access encrypted data if it has a key. Taking this further, the Bill also grants the power to compel companies to engage in actively building new tools and mechanism at the request of law enforcement agencies.

There is no warrant or oversight process here other than that these orders must be "reasonable and proportionate." While the government has pointed to the potential for people challenge in the courts, there is no outline of what this process will be or how the courts will be equipped to handle them. There is also the strong possibility that people will be prevented from revealing any information about any order they receive – with fines and jail time for those who do speak out.

The legislation also does not seem to be limited by what help organisations can be ordered to do. The government claims the legislation specifically forbids activities that would provide a 'systemic weakness or vulnerability' into an encrypted system. However, the kind of operation that the government is planning doesn't require an active creation of a weakness, instead opting for an end-point activation. Most encrypted services allow you to have multiple devices such as a phone and a computer, which can be end-to-end encrypted between all endpoints. If the government could secretly add a new device to that conversation without your knowledge, it would be building a new door into that encrypted communication.

Emily Olorin
[redacted]