From: Paul Arden
To: Assistance Bill Consultation
Subject: Feeback on Assistance and Access Bill 2018
Date: Monday, 10 September 2018 8:19:22 PM

To whom it may concern.

I am deeply troubled by the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 and the associated Fact Sheets which are clearly authored to provide reassurance despite there Bill itself being fundamentally flawed.

The stated aims are to enable law enforcement to access encrypted communication, somehow without creating systemic insecurities or weakening security of the systems that provide them. This is simply not possible, if it were the Bill should make clear what potential mechanisms could be used. The lack of such material shows that the authors of the Bill do not understand the fundamental nature of encryption and security.

Furthermore, the Bill is so broadly constructed that essentially any website that is accessible from Australia may be required to comply with it. Despite assurances it will not be used lightly there is no protection in law to prevent the relevant government parties from choosing the broadest interpretation possible.

Lack of oversight and reporting for the The Technical Assistance Request (TAR) is also particularly troubling given the broad applicability of this type of request. These requests do not have the same restrictions and while they are voluntary in nature the simple reality is that when law enforcement of government agencies wish to apply pressure to entities to comply, despite it being voluntary they can do so and the lack of oversight for this type of request makes it impossible for the public to understand what is happening.

The requirements imposed by this Bill will additionally stifle innovation and increase costs for affected entities who need to comply with the various types of requests and notices. In particular while provision is made for compensation the potential for exceptions have been allowed. Potentially forcing a business to choice compliance or ceasing operations due to being unable to meet the costs of compliant.

Companies operating in Australia will need to revise terms and conditions and legal agreements with customers to ensure they are aware that they may be compelled by the Australian government to comply with these types of requests. While most companies include a 'if required by law' clause, the expansive nature of the powers under this Bill are likely to cause greater customer concern and may even cause users overseas to reconsider utilising online services offered by Australian businesses, hurting our ICT export sector.

As a business owner and operator, even though one not directly offering communications services I find all of these items problematic. I also feel the Bill will simply not have the impact that law enforcement anticipates since as soon as it becomes clear where communication is compromised by government interference, parties will move their elicit activities to a platform which has not been compromised. There is no defence against end-to-end and at-rest encryption in which a provider has no access to what is needed to decrypt the communication, except in cases where there are abilities to break that encryption, which if implemented properly should not be possible.

Regards

Paul Arden