Brandon Butler

[redacted]

Department of Home Affairs

By website form

10 August 2021

Dear Sir/Madam

Response to the 'Strengthening Australia's cyber security regulations and incentives' discussion paper with respect to Australia's Cyber Security Strategy 2020

I refer to the 'Strengthening Australia's cyber security regulations and incentives' discussion paper with respect to Australia's Cyber Security Strategy 2020 (**the Cyber Security Strategy**) (**the Discussion Paper**).

First and foremost, I wish to express my utmost appreciation for seeking feedback from the public regarding cyber security policy and offering the opportunity to submit responses to the Discussion Paper. I am confident that my views are reasonably representative of my age group, Generation Z, who currently comprise predominantly of students completing secondary and tertiary levels of education and seeking employment in Australia's workforce.

As raised in the Discussion Paper, I am concerned that the goal with respect to cyber security policy to *'... make Australia's digital economy more resilient to cyber security threats'* and its intended means to achieve such goal by *'[creating] stronger incentives for Australian businesses to invest in cyber security'* is an unreasonable prospect.

The nature of the cyber security environment entails an inherent characteristic of investment in the sector having the same value as a 'blackhole'. I establish this comparison as the proactive approach that the Cyber Security Strategy proposes is economically unviable. Specifically, it ought to be understood that the cyber security environment is a contemporary discipline. Unlike the nature of conventional crime, the cyber security environment deals in a demographic that reaches worldwide talent in combination with the extensive innovative opportunities available with computers. Accordingly, investment in the cyber security environment with a proactive approach will continually and persistently demand increased funding, potentially carrying the regrettable consequences of depriving essential sectors of needs and exceeding the government resources that are available.

Mechanisms in the Australian justice system currently exist to administer criminal prosecution for people who breach cyber security laws. For example, unauthorized access to or modification of restricted data held in a computer constitutes a criminal offence that carries imprisonment in both Commonwealth jurisdiction under section 478.1 of the *Criminal Code Act 1995* (Cth) and NSW jurisdiction under section 308H of the *Crimes Act 1900* (NSW).

In *Roads and Traffic Authority of New South Wales v Care Park Pty Limited [2012] NSWCA 35*, the judgment found that use of a discovery order made upon a third party for the purposes

of determining the identity or whereabouts of a person may be done merely on the prerequisite that such information requested will aid the litigation process.

In *Dallas Buyers Club LLC v iiNet Limited [2015] FCA 317*, the judgment provided guidance on the interpretation of rule 7.22 of the *Federal Court Rules 2011* (Cth) with respect to the issue of to what extent a discovery order must identify a person for it to be a valid request for information to determine the identity or whereabouts of a person in the circumstance of an end-user of an internet service being a different person to the accountholder. Justice Perram stated: *'... it is difficult to identify any good reason why a rule designed to aid a party in identifying wrongdoers should be so narrow as only to permit the identification of the actual wrongdoer rather than the witnesses of that wrongdoing.'*

However, the commission of most cyber security incidents occur in foreign jurisdictions. This involves the exercise of document service and extradition powers in international law and coordinated effort between the Attorney-General's Department and diplomatic channels to negotiate the surrender of an alleged criminal overseas to administer criminal prosecution in this jurisdiction. Due to the potential lengthiness and expense risk with such means, such mechanisms are often reserved for allegations of crime considered to be serious only.

Therefore, I recommend that the Cyber Security Strategy instead considers applying a reactive approach to cyber security policy to impose accountability on organisations and government agencies who cause destruction to the economy consequential of overexposing business operations and infrastructure to computer systems unnecessarily. For example, the notorious Colonial Pipeline cyber attack in May 2021 caused worldwide news media to announce national economic damage to the United States in their capacity as the operator of a major petroleum pipeline and some motor vehicle owners to no longer be able to afford fuel due to inflated petroleum prices. Accordingly, Colonial Pipeline demonstrated negligence to exercise due diligence with recognition of their role in national economic performance when deciding to migrate business operations and infrastructure to rely completely on computer systems with no options to resort to if their computer systems were to malfunction.

If you have any queries regarding this letter, please do not hesitate to contact me on [redacted] or by email to [redacted]

Yours faithfully

[redacted]

Brandon Butler