To whom it may concern,

I am writing to submit comments to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) regarding the review being conducted on the Telecommunication and Other Legislation Amendment (Assistance and Access) Act 2018. I do so as a concerned member of the public.

For the last 17 years I have been professionally involved in the online digital space, ranging from ecommerce, startups to internet infrastructure & devops. I have seen the Australian digital industry mature & provide innovation as well as meaningful, gainful employment for many professionals across Australia, furthering more jobs & growth. It is my understanding as well as the understanding of many other experienced tech professionals from many sectors, both in Australia[1] & worldwide[2], that the Telecommunication and Other Legislation Amendment (Assistance and Access) Act 2018 needs to be significantly amended.

I will attempt to address the business, government & economic benefits of strengthening encryption instead of introducing "systemic weaknesses" prior to providing recommendations on amendments to this act.

SOFTWARE DESIGN

Software development best practice, from a monetary return on investment perspective, requires best practice principles to be set in place surrounding security of customer & business data. That data may include names, credit card & banking details, personal health data (such as in MyHealthRecord or ParentsNext). Australian technology industry professionals, be they working in ecommerce, government, startups, cloud based multinationals, all require the data they work with every day to be secure. If it is not secure, when that data is leaked/exposed across the Internet, the Office of the Australian Information Commissioner must be informed in line with the Notifiable Data Breaches scheme.[3]

---

[1] https://www.lowyinstitute.org/the-interpreter/disruptors-disrupted-australia-new-encryption-law

[2] http://fortune.com/2018/12/06/australia-encryption-law/

[3] https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

Furthermore, if these breaches affect European businesses & customers, due to Australian startups, businesses & multinationals doing international trade, that security breach may incur fines in line with GDPR regulations.[4]. Effective software design worldwide does not sacrifice security for convenience[5]. Numerous security breaches leaking personal data across the Internet, now ranging into the billions of users worldwide, show that encryption & security is not only big business, but also good business practice. This business practice helps foster GDP growth & innovation in Australia through startups, multinationals & the technology sector.

SYSTEMIC WEAKNESS

Introducing any form of systemic weakness into software developed in Australia, by Australians or for Australians also exposes that weakness to the rest of the world, even if unintentionally. This is how software attack vectors shown by information security experts such as Edward Snowden, are used at nation state level.

It would seem somewhat contradictory for a nation such as Australia to enforce privacy/security regulation through the OAIC & then let software used & developed by Australians to be a petri dish for offensive attack vectors against citizens in Australia as well as worldwide.

Government based projects such as MyHealthRecord & ParentsNext have already leaked citizen data, in addition to the metadata legislation now having over 1100 agencies/businesses accessing citizen data without consent or oversight. Adding in any further weaknesses to software design & development will only provide easier targets for other nation states & criminal enterprise to profit from misuse & mismanagement of data linked to Australian citizens. This not only lessens the standing of the Australian technology industry worldwide but also shows the apparent disregard some political parties & entities have for the integrity of Australian citizens' privacy.

---

[4] https://www.oaic.gov.au/resources/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation.pdf

[5] https://www.engadget.com/2018/02/16/how-security-became-more-important-than-convenience/

RECOMMENDATIONS

These are the recommendations for amending the Telecommunication and Other Legislation Amendment (Assistance and Access) Act 2018.

- The secrecy provisions in the Act must be removed.
- The Act must be revised to meet privacy standards present in OAIC & GDPR
- The notion of "systemic weakness" should be removed from the Act as any weakness will expose innocent citizens to the same exploits aimed at specific individuals or groups, raising further privacy concerns & possible attack vectors by unintended actors, be it individuals or other nation states.
- Any business or individual receiving a TCN should be recompensed at above industry pay rates for any changes to software required for that TCN.