Cortex I.T. Labs Pty Ltd submission:
Impact of new and emerging information and communications technology

Cortex I.T. Labs Pty Ltd
991 Whitehorse Road
Box Hill VIC 3128
Australia

Committee Secretary
Parliamentary Joint Committee on Law Enforcement
PO Box 6100
Parliament House
Canberra ACT 2600

12th January 2018

Dear Committee Secretary,

Re: Supplementary submission regarding the effect of forcing Australian technology companies to weaken the security of data protection products

This brief letter elaborates upon a previous submission made by Scram Software Pty Ltd.

We support the points made by Scram Software. However, we wish to add additional salient points based on our experience in developing and selling data protection software over the last 15 years.

We are a software company founded in 2001, and currently employing around 25 people in Melbourne and approximately a further 7 overseas. We develop and sell a product known as “BackupAssist”, which is a backup and disaster recovery software product aimed at the SME market. Essentially, the software allows users to take backups of their data and store them either on-premise, or in the cloud.

We protect our clients from data loss. For example, should their hard drive crash, or if they get infected by ransomware, they can restore their data or recover their entire computer system from a backup.

Our client base includes small and medium businesses across 165 countries, as well as government departments, charities, NGOs, and corporates. Given the sheer breadth of our client base, our software needs to support a wide variety of data storage targets, from on-premise storage (hard drives) to Internet based storage (public cloud and private cloud).

Encryption is a feature demanded by many of our clients. We were first asked for encryption by our American healthcare clients, who needed that feature to be “HIPAA compliant”.

Since that time, we have incorporated encryption into our product in three different ways:

1. implementing it directly in our software, where possible;
2. bundling our software with existing encryption systems, where option #1 was not possible, and finally,
3. teaching our clients how to use "Bitlocker" full disk encryption, an existing feature built into the Microsoft Windows Operating System, when options #1 and #2 were not possible.

In all of these options, each client manages their own encryption key – a key requirement for security and compliance with data sovereignty laws.

The backup and disaster recovery software market is saturated with options. We have dozens of direct competitors from various countries around the world, and encryption is a core feature of all of our competitors.

Our position, as a software vendor, is best illustrated with several examples:

- When an American hospital, subject to American HIPAA regulations, uses our software to back up patient data to an American data centre, using encryption keys that they created, we neither have access to the data nor the encryption key.

- When a Finnish education provider, subject to the EU's GDPR, uses our software to back up student details and grades, to a hard drive that gets stored in a safe located onsite, using encryption keys that they created, we have neither access to the data nor encryption key.

- When a Canadian accountant, subject to Canadian PIPEDA regulations, uses our software to back up their client data and financial records to a NAS device on their network, using encryption keys that they created, we neither have access to the data nor the encryption key.

- When a Singaporean lawyer, subject to Singaporean PDPA regulations, uses our software to back up their client data and files to a local hard drive, using encryption keys they created, we neither have access to the data nor the encryption key.

In all cases, the data that our software backs up and encrypts is none of our concern. Our software is free from spyware and must continue to be in order for us to maintain trust in the marketplace.

Cortex I.T. Labs Pty Ltd submission:
Impact of new and emerging information and communications technology

Our customers, both businesses and governments, require guarantees of data privacy and sovereignty. If we were forced to introduce any backdoor, or otherwise weaken our software, all it would do is force our customers to choose alternative solutions from vendors located in other countries that place no such onerous restrictions. Naturally, if we lose our customer base, we will be forced to close our business. The current speculation over encryption, backdoors, weakened security, and similar topics, currently represents one of the most significant risks to the viability of our company, and the job security of our employees.

Yours faithfully,

Linus Chang

Director
Cortex I.T. Labs Pty Ltd

Steven Chua

Director
Cortex I.T. Labs Pty Ltd