SCRAM SOFTWARE
SECURING YOUR DATA IN THE CLOUD

Scram Software Pty Ltd
Suite 410, 365 Little Collins Street
Melbourne VIC 3000, Australia
www.scramsoft.com

Linus Chang
Director, Scram Software

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

11th January 2018

Dear Committee Secretary,

Re: Flow-on effects of regulatory requirements governing encryption on cyber-security businesses in Australia

I thank you for your invitation to make a submission to your committee.

My concerns are to highlight to your committee the possible flow-on effects of possible "bans", "backdoors" or other "weakening" applying to encryption technologies developed by Australian cyber-security companies such as my own, and the effect it could cause on export sales and employment.

I shall divide my letter into four parts:

1. The cyber-threat landscape
2. My background – who am I?
3. The worldwide stance on encryption and the business opportunity
4. The commercial effects of weakening security

1. The cyber-threat landscape

As is frequently reported in the news, cyber-crime and data breaches are becoming more frequent and more severe. The use of technologies such as cloud computing, biometrics, genomics, big data, to name a few, have meant that more and more sensitive information is stored digitally, on servers that are vulnerable to attack.

In addition, human error also results in data breach. A good example of such a data breach that's close to home is the 2016 Red Cross Blood Bank breach, where details of 550,000 blood donors, (including names, addresses and details of *at-risk sexual history*) were leaked because of human error when a database backup was placed on a public facing server. If you donated blood in the last 5 years, the chances are that your details were leaked.

Our encryption software would have prevented that.

SCRAM SOFTWARE
SECURING YOUR DATA IN THE CLOUD

Scram Software Pty Ltd
Suite 410, 365 Little Collins Street
Melbourne VIC 3000, Australia
www.scramsoft.com

Without our technology, these kinds of data leaks and breaches are only going to get worse and worse. In October 2017, the world learnt about South Africa's largest data breach (of 66,360,837 records), affecting almost every citizen. The breach included ID numbers, age, location, martial status, estimated income, physical address and cellphone numbers. All information came from a database backup, leaked by a real estate company. Somehow, the backup was placed on a public-facing web server.

Again, our encryption software could have prevented that.

2. My background – who am I?

I'm an Australian software developer and entrepreneur, born in Melbourne. I currently have two businesses employing around 30 in Melbourne and more overseas. It all started back in 2001 after I quit my job as a software developer, and created my own enterprise. I developed a backup software product, BackupAssist from my bedroom and selling it via the Internet while I was living off savings. Since bootstrapping my business from nothing, I've built a great team, and our software is sold in 165 countries to every form of business, government and non-profit, with clients including the Department of Homeland Security, NASA, NATO, Pfizer, MIT, Harvard University, and hundreds of thousands of others. Today, BackupAssist is a popular program used to prevent data loss and negate the effects of ransomware.

95% of sales are exports.

Several years ago, I started to get concerned about hacking and data theft in the age of the cloud. I saw cyber-crime as a huge and growing problem. Therefore, I started another venture, Scram Software, in 2014, specializing in cyber-security using encryption.

Over the next 3 ½ years, I assembled an amazing team, partnering with cryptographers and security researchers at Monash University and the University of Melbourne, as well as employing PhD candidates and graduates, and providing studentships for Masters students from those universities. We've even achieved some world-firsts in the field.

Now my new business, Scram Software, is now on the verge of launching our flagship product. It is a product that should help companies and non-profits worldwide secure sensitive data from breach.

If successful, I'm sure my company will also be a poster child for Australian innovation – a successful partnership between industry and academia leading to innovative technology that gets exported to the world.

3. The worldwide stance on encryption and the business opportunity

The opportunity for Scram Software is considerable given that we have developed unique encryption technologies to protect sensitive and private data.

SCRAM SOFTWARE
SECURING YOUR DATA IN THE CLOUD

Scram Software Pty Ltd
Suite 410, 365 Little Collins Street
Melbourne VIC 3000, Australia
www.scramsoft.com

One should note that legislation worldwide either mandates the use of encryption (such as Australia's Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015) or refers to encryption in highly favourable terms as a method to prevent data breach.

In particular, Europe is going to be a huge market with legislation such as the EU's General Data Protection Regulation (GDPR) making our technologies appealing for safeguarding private data. Encryption is specifically referred to as a recommended safeguard in GDPR Article 32. All companies that collect or process data on EU residents must comply with GDPR, no matter where the company is domiciled.

The USA safeguards medical data though HIPAA legislation, "protected health information" (PHI) must be safeguarded for confidentiality and integrity (ref. § 164.306 Security standards: General rules). Entities covered by HIPAA must demonstrate appropriate safeguarding, with encryption cited as a mechanism (ref. § 164.312 Technical safeguards).

We anticipate that 95% of sales would be exports, just like in my first business.

Furthermore, our technologies can also be extended to solve issues such as invoice fraud and authenticated document sharing and delivery. A few months ago, a friend of mine in Melbourne who runs a marketing company lost tens of thousands of dollars when her business' server was hacked and invoices were altered with changed bank account details. She reported the incident and was issued an ACORN reference number, but the allocated law enforcement agencies are so inundated with reports like this, she had to seek private help with her situation. This is the kind of cyber security solution that we want to work on, and with our solid encryption platform we are well placed to solve that problem.

We also believe we could fight ransomware with our system. Given some time, and even some support from the Australian Government, we could be a major player in the fight against these 21st century threats.

Finally, we believe that our systems would be highly useful for Australian law enforcement agencies, safeguarding highly sensitive data and mitigating the likelihood of data leaks and exfiltration, especially when relating to data stored in the cloud.

4. The commercial effects of weakening security

I can report that based on my informal discussions with I.T. business people in Switzerland and Germany, Australia currently has something of a neutral reputation when it comes to trustworthiness in security products. This is because Australia has not (unlike other countries) had a high-profile track record of intentionally weakening security products.

I note that in the media that there is some discussion about encryption, but I have not seen any specific details about what is being contemplated. Presumably it relates somehow to weakening, wiretapping or insertion of backdoors.

SCRAM SOFTWARE
SECURING YOUR DATA IN THE CLOUD

Scram Software Pty Ltd
Suite 410, 365 Little Collins Street
Melbourne VIC 3000, Australia
www.scramsoft.com

I wish to point out that there are many different types of encryption, used for different purposes. In the case of our software, the client (i.e. the purchaser of the software system) owns their own data, they choose where to store it, and they have possession of their own encryption key (or password). There are issues such as data sovereignty that we need to abide by – for example, a German client would want to store their data in Germany, and keep their encryption key solely in their possession.

The fact that our systems are "clean", free from spyware and backdoors, and have been independently verified by cryptographers from Monash University and The University of Melbourne, is essential in building trust in the marketplace.

If we are forced to intentionally weaken the security of our software, we fear a devastating commercial effect as we would lose potential export sales due to mistrust in an Australian product. It would put Australian companies at a huge (if not insurmountable) competitive disadvantage compared with European companies.

In a worst-case scenario, we wouldn't be able to win customers and we'd be forced to close our doors before we even got started. My other business would also be affected, as encryption is a key feature of our backup software, required for us to sell into Europe and USA, thus putting ~30 Australian jobs at risk.

I believe the best way forward would be for the Australian Government to support its technology and innovation sector by providing certainty and collaboration with industry. In particular, commercially we **need** to be on a level playing field with our competitors in Europe. We also want to and have the opportunity to grow Scram Software into a world-renowned leader in cyber security, and be an export success story.

I also request that this situation be resolved with clarity from a legislation viewpoint, and a clear position on the matter be articulated. As the owner of small businesses, I need to be spending time and money on R&D and marketing, not on obtaining complicated legal advice.

Finally, I would like to reiterate to the committee my concern regarding the implications and potential competitive disadvantage that could be placed upon Australian companies like mine, and consequent effects on innovation and jobs. I would welcome every opportunity to work with our Government to help create an export success story and to create hi-tech jobs in Australia.

Yours faithfully,

Linus Chang