

Why we need to fix encryption laws the tech sector says threaten Australian jobs

Written by Damien Manuel, Director, Centre for Cyber Security Research & Innovation (CSRI), Deakin University

Australia's technology sector is [angry](#) . This is because Australia's encryption legislation clearly shows the government's lack of understanding and poor consultation process with the wider public and industry stakeholders, big and small.

The [Telecommunications and Other Legislation Amendment \(Assistance and Access\) Act 2018](#) – or TOLA for short – was passed late last year by the Coalition with Labor's support, [despite concerns](#) .

At the Safe Encryption Australia forum in Sydney this week it became clear the Morrison government [didn't even consult](#) with some of Australia's top tech businesses such as Senetas and Atlassian.

Read more: [*How big tech designs its own rules of ethics to avoid scrutiny and accountability*](#)

The [Parliamentary Joint Committee on Intelligence and Security](#) has [referred the TOLA](#) to the Independent National Security Legislation Monitor for review and report.

Based on the conversations at the forum, it is evident the Australian tech sector continues to haemorrhage.

Francis Galbally, non-executive chairman of Senetas, [said](#) "this legislation will force our company to go offshore".

Atlassian cofounder and co-CEO Scott Farquhar [added](#) : "We've got to recognise this law threatens jobs."

Why we need to fix encryption laws the tech sector says threaten Australian jobs

Written by Damien Manuel, Director, Centre for Cyber Security Research & Innovation (CSRI), Deakin University

This sentiment highlights the seriousness and the economic threat the legislation poses to our developing tech sector, and Australia.

After June 30, the Home Affairs Minister must produce an annual report outlining the number of times the Act has been used. So why are people so angry and what does it mean for Australians?

What is the TOLA?

The TOLA seeks to prevent terrorists, paedophiles and other criminals communicating in secret, without law enforcement and security agencies being able to “[crack their code](#)”, as put by Mike Burgess, director-general of the Australian Signals Directorate.

The act attempts to do this by requiring a provider to do things to assist certain agencies. This can include removing electronic protection (authentication and encryption), providing technical information to subvert protection, facilitating access to information, installing software or equipment, and concealing the fact anything has been done.

The Act can be used for “serious Australian offences” that are punishable by a maximum term of imprisonment of three years or more.

Under this definition, the Act can be used against people suspected of internet trolling, attempting to disrupt electronic communications, people growing marijuana for the purpose of trafficking, or those suspected of theft or recklessly causing injury.

If the law was really intended to catch paedophiles as the government stated, rather than mass surveillance of large segments of society, why wasn't the benchmark of serious crime set to [ten years which is the maximum term](#) for knowingly possessing child pornography? Why is the bar set so low?

How does the TOLA impact you?

Trust in the devices and technology we use on a daily basis is key for both consumers and

Why we need to fix encryption laws the tech sector says threaten Australian jobs

Written by Damien Manuel, Director, Centre for Cyber Security Research & Innovation (CSRI), Deakin University

producers of the technology. Trust is achieved by knowing your data, photos and personal information are not accessible by anyone without your knowledge and that the providers of the services you use, will protect your data and information.

Essentially, your privacy is respected. With the TOLA, you now have no privacy when it comes to your online information and any technology you use.

It is like giving the government a key to your house, so they can come in anytime, without proper judicial oversight and go through all your things, just in case you might be a terrorist or a criminal.

If you work for a company or provider who is requested to assist under the Act and you disclose that information to anyone who is not authorised to know, you can go to prison for five years.

Unlike the European Union and United States, which have provisions to protect the privacy of their citizens and prevent government overreach, Australia unfortunately has none.

Can criminals and terrorists get around the Act?

The simple answer is yes. Anyone, even law-abiding Australians, can get around the new laws by using one or more of the following techniques:

1.

Use apps that are outside the jurisdiction of the Australian government. These will typically be produced by organisations based in countries Australia has no influence or agreement with making the law harder to enforce.

2.

Buy a Virtual Private Network (VPN) service that ensures point-to-point encrypted connections with no logging.

Why we need to fix encryption laws the tech sector says threaten Australian jobs

Written by Damien Manuel, Director, Centre for Cyber Security Research & Innovation (CSRI), Deakin University

3.

Download and start using the Tor browser, a free and open-source browser for enabling anonymous communication. Tor was originally designed by the US Naval Research Laboratory to protect US intelligence communications online.

A major consequences of the Act is that it now incentivises criminals or terrorists to use these and other methods to evade detection. Worse still, it encourages them to build their own tools, making it even harder for law enforcement to find, monitor and track them.

Who is to blame for this mess?

First to blame is the Morrison government for rushing through Parliament poorly written legislation. Second is Labor, for helping the government pass the legislation.

The Shadow Minister for the Digital Economy, Ed Husic, [told the forum](#) Labor passed the laws with a view to making amendments in 2019.

“Our view was to give something to the security agencies in the short term”, he said.

But really, is that any excuse for helping to pass legislation that is causing uncertainty and doubt for Australia’s tech sector and their local and international customers.

Read more: [Why new laws are vital to help us control violence and extremism online](#)

Why we need to fix encryption laws the tech sector says threaten Australian jobs

Written by Damien Manuel, Director, Centre for Cyber Security Research & Innovation (CSRI), Deakin University

Husic [also told the forum](#) Labor was now committed to “fix these terrible laws”.

But this will take time our newly developing tech sector and established businesses cannot afford as they lose revenue and customers.

The right thing to do by Australian businesses, before they move offshore, is to repeal the legislation. Helping to keep Australia globally competitive, restoring confidence in our tech sector and respecting the Australian community would be a refreshing change.

Damien Manuel is affiliated with AISA (Australian Information Security Association) as the chair, Oceania Cyber Security Centre (OCSC) as a director (representing Deakin University), mentor for CyRise founders (representing Deakin University), CompTIA as an exam writer and on the CompTIA Executive Advisory Committee in the USA and as an expert on the Standards Australia Committee for Information Security (IT-012).

Authors: Damien Manuel, Director, Centre for Cyber Security Research & Innovation (CSRI), Deakin University

Read more <http://theconversation.com/why-we-need-to-fix-encryption-laws-the-tech-sector-says-threaten-australian-jobs-110435>