Big Brother is watching: Australia's 'snooper's charter' is now law.

If you're working in the technology sector, or you use iMessage, WhatsApp or any other encrypted messaging service at home or in your business – you'll want to read this.

Yesterday evening the government passed the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*. Modelled on the UK *Investigatory Powers Act 2016*, the Australian government, together with the Labor opposition has handed the security services the Western world's most extensive cyber-surveillance powers.

Why? The government says the law is a response to the impediment that the increasing prevalence of encrypted data and communications represents to the investigative and interception capabilities of our security agencies.

In short, too many terrorists and criminals are using encryption to evade monitoring by the Australian Security Intelligence Organisation and the Australian Federal Police. These agencies, together with their Five Eyes counterparts (in Canada, New Zealand, the United States and the United Kingdom) want the ability to compel technology companies to assist the security agencies by breaking their own encryption to allow access to private communications.

For their part, technology companies, industry groups and civil libertarians are united in their stance that this is a pretty terrible new law. They say that ordering 'designated communications providers' to break or weaken encryption will make cyberspace more dangerous for everyone. The government was warned that weakness in encryption can not only be exploited by the good guys, but the bad guys too. They didn't listen.

So, what Orwellian dystopia do we have to look forward to?

'Voluntary' assistance and encryption ~~weaknesses~~ capabilities

Government agencies now have the power to issue requests for voluntary assistance (technical assistance request). If the designated communications providers (tech companies and network operators) refuse, they can be compelled to provide assistance or build a new encryption back-door (technical assistance notice and technical capability notice). However, the government says these technical capabilities are absolutely not systemic weaknesses. Double-speak if we've ever heard it. Orwell would be spinning in his grave.

Limited judicial oversight

The oversight of the compelled assistance and capabilities will be limited, with providers able to appeal to a retired judge and an industry expert for an adjudication where they believe a capability will create a systemic weakness in their encryption product. Oh, and the whole process is subject to absolute secrecy.

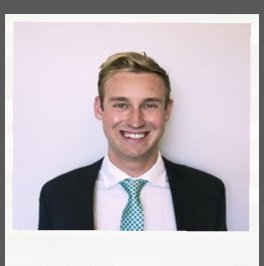
Amongst the other concerns raised by industry (think: Atlassian, Apple, Mozilla) and the Law Council of Australia, are:

1. The significant scope for abuse of broad and ill-defined new powers;

2. It is unclear if end-to-end encryption may actually be offered by tech companies and if they would still be able to comply with the law; and

Jennifer Johannesen
Senior Associate

+612 8216 3033
Email Jennifer



Lachlan Blair
Paralegal

+612 8216 3036
Email Lachlan

Marque Lawyers Pty Ltd
Level 4, 343 George St
Sydney NSW 2000

Ph : +61 2 8216 3000
Fax: +61 2 8216 3001

Visit Website

Concerned? Confused about how your company can comply?
Questions? Give us a call.