Government Bill opens the back door for hackers

OCTOBER 3, 2018

Not long after Scott Morrison swept aside the cybersecurity ministry to make way for his newly formed cabinet, the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* was introduced to Parliament. While the Bill may sound innocuous, its scope and implications could significantly impact personal data security in Australia and make it easier for hackers to access personal data stored on devices.

What does the Bill do?

While two thirds of the Bill is aimed at providing law enforcement agencies with the power to compel suspected criminals and terrorists to provide access and passwords to personal devices to assist with an investigation, it is the "technology capability notices" that are the most contentious.

Companies that provide communication platforms rely on end-to end encryption to protect customer data from hackers. While acknowledging encryption makes it harder for hackers, the government says that this level of encryption also impacts approximately 90% of ASIO investigations.

To address this it introduced the Bill, which gives new powers to law enforcement agencies to compel companies to provide access to encrypted communications where they are needed to fight cybercrime and terrorism. The Bill has broad application and will affect local and multinational telecommunications companies, internet service providers, device manufacturers, social media platforms and email providers.

The Bill empowers law enforcement agencies to compel those companies to do a wide range of "acts or things". For example, agencies might ask a company to remove electronic protection from stored information, install software or give access to a device. Agencies could also ask companies just to ensure they could do these things, if requested. What's more, the proposed powers are so broad that agencies can request access without any judicial or independent oversight.

Potential impact

While the Bill specifically does not require companies to take actions that would build weaknesses into their systems, in practice it is possible that could happen. Technology commentators say it will be impossible to comply with the Bill while protecting data with end-to-end encryption. If that is the case, then the Bill must inevitably require companies to relax their encryption. In turn, this would create system back doors for law enforcement that could also be exploited by hackers.

The Bill is modelled on its UK equivalent, the *Investigatory Powers Act 2016*. It was successfully challenged in the courts earlier this year for breaching the right to privacy under EU law, which notably is rights-based. In contrast, the Australian *Privacy Act 1988* focuses on the protection of the data rather than the rights of the individual, so it is unlikely an Australian court would make a similar ruling. However, the UK decision remains a concern in the context of the Australian approach.

So what rights are we concerned about? Do Australians really care if their WhatsApp conversations and Facebook photos are shared with government agencies, and potentially exposed to hackers, given the trade-off helps authorities fight cybercrime and terrorism? It's hard to know. But it is reasonable to assume they would be concerned about protecting passwords and other sensitive or valuable information, which is stored on their devices and apps.

The friction between data privacy and law enforcement is more prevalent than ever. Even if the Bill fails to pass through Parliament on this occasion, it appears to signal a policy shift by the government in favour of national security over individual privacy. While no one can doubt the importance of enabling law enforcement with a greater ability to fight crime, it comes at a time where data breaches are now a feature of the connected world we live in and the risk to data privacy is more prevalent than ever before.

W+K Contacts

For more information please contact:

Kieran Doyle
Special Counsel, Sydney
+61 2 8273 9828