HERBERT SMITH FREEHILLS

THE ASSISTANCE AND ACCESS ACT 2018: THE CRYPTO WARS' FINAL ACT FOR 2018

11 December 2018 | Australia
Legal Briefings – By **Julian Lincoln, Anna Jaffe and Lara Howden**

On 6 December 2018 — the last sitting day of Parliament of the year — the Federal Government passed the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth), which received Royal Assent earlier this week (the **Act**).

The Act amends the *Telecommunications Act 1997* (Cth), among other Acts. The features of the Act that have captured the most public attention relate to the frameworks established in the Act for law enforcement and intelligence agencies to make voluntary and mandatory requests for the provision of industry assistance, via what are referred to as 'technical assistance requests', 'technical assistance notices' and 'technical capability notices'.

WHAT PROMPTED THE ACT?

WHY WAS THE ACT INTRODUCED?

The Act's purpose is to assist law enforcement and intelligence agencies to continue to perform their authorised functions in the face of increased technological barriers caused by widespread public adoption of certain technologies, including encryption.

The Act aims to:

- recognise that these agencies' legal authorisation to access information and communications, and otherwise perform their authorised functions, is often undermined by their limited technical capacity to do so (for example, through increased use of encrypted communications by the targets of investigations); and

- reinforce, and enhance, these agencies' technical capabilities when they are already legally authorised, by securing the technical assistance of private companies in the communications and technology industries (which are broadly defined and referred to in the Act as 'designated communications providers').

The Act was initially introduced into the House of Representatives on 20 September 2018, and was rapidly passed into law following a period of consultation and consideration by the Parliamentary Joint Committee on Intelligence and Security, largely in response to perceived heightened security risks around the impending holiday period. The introduction and passage of the Act, including the circumstances in which it was passed into law, have not been without controversy.

HOLD ON, HAVEN'T I HEARD THIS BEFORE?

The tension between national security interests and the public interest in privacy, security and confidentiality of communications is not a new one, but has reared its head again in this debate.

In the 1990s, the 'Crypto Wars' over access to encryption were prompted by similar concerns of lost access to communications in the face of new technologies, and were ultimately abandoned due to widespread public opposition. In this decade, law enforcement and intelligence agencies, from the United States FBI to ASIO, have long warned of a surveillance environment that is 'going dark' (in other words, a technological environment that is not capable of interception). These warnings have resurfaced following terrorist attacks (both actual and intended) in San Bernardino, California and this year in Melbourne, where perpetrators used encrypted messaging applications to communicate. The attack in San Bernardino itself prompted the FBI to request a court order seeking technical assistance from Apple in helping to circumvent the security features of a device used by one of the perpetrators of that attack, a request that Apple rigorously and publicly defended.

Conversely, although these sentiments have led to calls to weaken encryption in order to better target terrorist threats and other serious crimes, many industry participants have argued that stronger — not weaker — encryption is the answer. For example, consider the revelations of mass surveillance and interception capabilities of government authorities as revealed by Edward Snowden and Wikileaks, which prompted technology providers to address users' growing mistrust in the security of their personal data by introducing increased security features on devices and services. These features, such as end-to-end encryption from sender to recipient and device-based encryption of locked devices (often enabled by default), served to reassure users that no one, not even the providers themselves, could access their data.

Out of these two opposing views, government and industry have sought to find a way through the 'going dark' problem that does not compromise the benefits of strong encryption to the public. The need for specialist technical assistance from industry has been on the agenda of the Governments that are part of the 'Five Eyes' intelligence network (of the United States, the United Kingdom, Canada, Australia and New Zealand),[1] and has ultimately led to the introduction and passage of the Act.

WHY HAS THE ACT LED TO SUCH CONTROVERSY?

The Act allows law enforcement and intelligence agencies to both request and compel technology companies and communication providers to do certain 'acts or things' in order to enable those agencies to access communications, including encrypted communications.

The Act prompted a number of submissions from industry participants, who argued that although the Act was intended to require industry assistance in accessing data only in respect of *targeted* individuals (and their devices and technology), the form of assistance required could mean that providers were forced to modify their products and services by building and introducing weaknesses and vulnerabilities into them, which could then be exploited by the relevant agencies. One key problem with this situation is that weaknesses applied to one device may have any number of unintended consequences, such as:

- any unpatched weakness or vulnerability, even if only intended for one system, is likely to be capable of being applied to other systems if and when it is discovered (and could therefore affect non-targeted users and systems, or the security of systems generally); and
- newly built capabilities (including weaknesses and vulnerabilities) may not be extensively tested given the time pressures imposed for industry assistance and restrictions on disclosing information in relation to requests and notices, and could have unknown consequences for both the relevant system(s) as well as other systems and devices in the supply chain.

The Act sought to address the issue of the potential broader consequences of weaknesses and vulnerabilities by prohibiting the introduction of a 'systemic weakness' into a form of electronic protection. This prohibition also expressly prohibited the implementation or building of decryption capabilities, or rendering 'systemic methods of encryption less effective'.[2] In the version of the Act introduced into Parliament, the terms 'systemic weakness' and 'systemic vulnerability' were not defined, and definitions were only added on the day of its passage. These newly defined concepts relate to:

- whether or not a weakness or vulnerability is ‘selectively introduced to one or more target technologies that are connected with a particular person’ rather than affecting a ‘whole class of technology’;

- the term ‘target technology’, which then considers whether the relevant services and devices are ‘used, or likely to be used, (whether directly or indirectly) by a particular person’; and

- whether the acts or things undertaken by a provider will, or are likely to, 'jeopardise the security of any information held by any other person’ (which echoes comments made by the Australian Signals Directorate in hearings in relation to the Act). This is further clarified to occur ‘if the act or thing creates a material risk that otherwise secure information can be accessed by an unauthorised third party’.

These concepts, although more useful than the limited treatment of ‘systemic weakness’ and ‘systemic vulnerability’ in earlier drafts of the Act, are likely to be subject to differences in interpretation, particularly as the relevant technology continues to evolve.

In any event, many industry participants argued (and continue to argue) that these prohibitions were insufficient on their own, and were compounded by other issues present in the Act, including:

- concerns that the definition of 'systemic weakness' introduced on the day of its passage is not adequate, and accordingly there is a risk that the new powers given to law enforcement and intelligence agencies could inadvertently lead to the weakening of encryption that protects critical and legitimate infrastructure;

- the safeguards in place for these frameworks, given the diverse range of agencies that may utilise these powers, are not sufficient (including that many decisions made under the Act are not subject to independent judicial review); and

- the mere existence of the Act, and the powers within it to compel industry assistance subject to secrecy obligations, has the potential to damage the reputation of entities that are covered by the Act (including Australian companies) and seek to sell purportedly secure products and services, even when they have not been directly subject to any requests or notices under it.

Ultimately, this is not the end of the road for the Act, as its passage was secured only with the promise of further review and requests for amendment by the Federal Opposition. The Parliamentary Committee of Inquiry will commence a review of the new legislation and hold further public hearings, with a view to completing the legislative review by 3 April 2019.

ENDNOTES

1. See Statement of Principles on Access to Evidence and Encryption, available here.
2. The Act, Sch 1, s 317ZG.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

JULIAN LINCOLN
PARTNER, HEAD OF TMT & DIGITAL AUSTRALIA, MELBOURNE
+61 3 9288 1694
Julian.Lincoln@hsf.com

LEGAL NOTICE
