Proceedings of the 3rd International Conference on International Law and Legal Policy
DOI: 10.54254/2753-7048/53/20240056

Australian Anti-encryption Legislation and Its Impacts on Security and Privacy

Yue Zhao[1,a,*]

[1]*Department of Online Operation, Industrial Bank of China, YinCheng Rd, Shanghai, China*
a. yzha4885@outlook.com
**corresponding author*

Abstract: *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* gives relevant authorities (e.g. law enforcement, national security agencies and intelligence agencies) significant new powers regarding access to encrypted communications data, and hence extensive public attention have been attracted and opinions expressed concerning general security and privacy of users. This essay will first briefly introduce the key contents of the *Assistance and Access Act 2018*, then discuss how it will affect security and privacy of users respectively by considering both supporting and opposing arguments, and then further the discussion into a global environment by examining the history of a variety of efforts on similar powers. It concludes that though the *Assistance and Access Act 2018* has sophisticated oversight mechanism and takes into consideration the most concerned systemic weaknesses security issue, its definition and guidance are vague and is likely not practical to achieve what the Act is designed for in practice. The potential overreach of the Act not only will impose great threats to system security as a whole, but also will breach the principle of privacy.

Keywords: Anti-Encryption, Security, Privacy

1. Introduction

In December 2018, the Australian parliament passed a new legislation *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (also known as the Assistance and Access Act or referred to as the Anti-Encryption Act). Relevant authorities (e.g. law enforcement, national security agencies and intelligence agencies) were given significant new powers by this Act regarding access to encrypted communications data, and hence extensive public attention have been attracted and opinions expressed concerning general security and privacy of users. Because of the great potential risks to the public, the introduction of the Act is very controversial. This essay will first briefly introduce the key contents of the *Assistance and Access Act 2018*, then discuss how it will affect security and privacy of users respectively by considering both supporting and opposing arguments, and then further the discussion into a global environment by examining the history of a variety of efforts on similar powers.

DOI: 10.54254/2753-7048/53/20240056

2. Key contents of the *Assistance and Access Act 2018*

Assistance and Access Act 2018 grants law enforcements lawful power to compel technology companies, either domestic or international, with providing assistance relating to access to devices and encrypted communications data [1]. There are three key powers granted to law enforcements under this Act. First, section 317A introduced a technical assistance request for law enforcements to seek voluntary help from designated communications providers that may involve technical details of online service development. Second, a technical assistance notice, once given, communication providers must provide assistance to law enforcements in relation to eligible activities of the provider, as set out under section 317L. For example, decrypting a particular communication is included as such an activity [2]. Third, section 317T established a technical capability notice to ensure law enforcements get listed help from designated communications providers in relation to the performance of a function.

3. Security concerns

The most concerned and discussed issue is security because of the potential formation of electronic protection, also known as 'backdoors' for data encryption. There has been a large amount of opposing voices worldwide regarding the vulnerabilities such decryption may create for the system as a whole. Effects of such access were examined extensively, and numerous negative consequences have been found on security.

IEEE [3] opposes exceptional access granted to law enforcement and other governmental agencies to encrypted data regardless of the intention, by stating that such mechanism would attract great threats by invoking systematic weaknesses and creating opportunities for hackers.

A group of computer scientists examined from technical perspective and supported their argument with further studies. They reported that by introducing exceptional access to the system, it increases its complexity which invites vulnerabilities, and hence granting government exceptional access to encrypted communications data is not feasible in practice without causing vulnerabilities in the entire system [4].

European Union Agency for Network and Information Security [5] also analyzed the technical possibility of providing a back door for law enforcement to gain access to encrypted communications data, taking into consideration of both digital signatures and authenticity, and concluded that although it is technically possible, such approach, similar to reducing the key size of encryption and decryption process, could reduce digital signatures' reliability by weakening encryption technology, lower public trust in relevant services by giving them an impression that their privacy is under surveillance, and hence undermine the security level on the whole industry.

Kopsias [6], a member of the NSW Police Force and Law Society's Privacy Law Committee, commented that, though the 'systemic weakness' is strictly prohibited by the Act, the definition is very vague, and guidance is insufficient as to how the law will be implemented in practice and how communications providers are able to satisfy requests without introducing a systemic weakness.

In summary, opposing arguments of the *Assistance and Access Act 2018* concerning security issue include systematic weaknesses and vulnerabilities it may create by introducing exceptional access and decryption, more opportunities for hackers' attacks, weakened encryption technology and public trust, and vague guidance provided by the Act in practice.

On the other hand, the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* includes a wide range of safeguards to oversee the implementation of the Act. And some government departments have responded to some key popular opposing arguments.

Schedule 1 Part 1 Division 7 of the Act includes oversight mechanisms. Section 317ZG of the *Assistance and Access Act 2018* establishes the boundary and prohibits requests that would cause

DOI: 10.54254/2753-7048/53/20240056

'systemic weakness or systemic vulnerability'. Sections 317ZGA and 317ZH set limits on requests and technical capability notices such as construction of new decryption capabilities. Sections 317WA and 317YA further assists the application of Division 7 by appointing assessors and establishing relevant rules of assessment and report. Section 317JAA and section 317P stated that request must satisfy technical feasibility.

Shortly after the Act passed the parliament, Mike Burgess, Director-General of Australian Signals Directorate made a statement regarding the Act and addressed some popular yet inaccurate commentary in the statement. With respect to the security concern, Mike Burgess [7] re-iterated the term 'systemic weaknesses' from the *Assistance and Access Act 2018* and said that this is explicitly prohibited by the Act and hence will be avoided with an analogy of entering a locked room in a hotel for anti-terrorist purpose and not demanding a master key for all rooms.

In response to many negative feedbacks, later in early 2019, the Department of Home Affair interpreted the *Assistance and Access Act 2018* with respect to several popular concerns. Firstly, regarding information security, the Department of Home Affair [8] interpreted that attempts to weaken the system as a whole and consequently jeopardize the security of general users is strictly prohibited under the Act, and this Act does not compel companies to build capabilities of removing protection. Secondly, regarding potential sensitive information and capabilities leakage, Department of Home Affair [8] responded that strong cyber security protocols implemented by both law enforcement and security agencies will be able to protect.

Both the Director-General of Australian Signals Directorate and the Department of Home Affair responded to the most concerned security issue and reassured that no systemic weaknesses will be created because it is strictly prohibited under the Act, and that strong cyber security protocols used by law enforcements will protect information and capabilities leakage.

4. Privacy concerns

Apart from security, encryption is also critical to a private and confidential communication. With encryption and decryption regulated by the newly passed *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, privacy issue raised controversial opinions over the Act.

One main opposing opinion is that, the Act, by allowing decryption of communications and granting access to encrypted data to law enforcements, poses threats to personal privacy. Law Council of Australia [9] President, Morry Bailes said that Australian's rights can be potentially compromised as the possibility of law enforcement overreach exists. Senator Jordon Steele-John also pointed this out in one of his speeches that Australian citizens' online privacy would be jeopardized because the principle of end-to-end encryption is undermined, and this new legislation is a direct overreach of people's desire to private data safety [10]. The Law Council of Australia [8], after serious evaluation of the legislation, continued to hold a concern with respect to impacted privacy, and extended affected groups from individual Australian citizen to media and corporate sector, which was also discussed in a review by the Parliamentary Joint Committee on Intelligence and Security with a solution regarding unauthorized disclosure of information. More importantly, the Act could also lead to a breach of General Data Protection Regulation – a privacy measure of the European Union. In summary, a variety of stakeholders hold an opinion that the *Assistance and Access Act 2018* compromises users' privacy due to the potential law enforcements' overreach of the legal powers and the overreach of private data safety principle.

The Director-General of Australian Signals Directorate and the Department of Home Affairs also responded to the privacy issue. The *Statement of Principles on Access to Evidence and Encryption*, though acknowledges the importance and necessity of privacy, and the commitment to personal rights, states the need of a compromise in privacy in the face of threats to national security [11], based on

DOI: 10.54254/2753-7048/53/20240056

which the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* introduces the lawful access to encrypted data for law enforcements.

Director-General of Australian Signals Directorate Mike Burgess [7] acknowledged the importance of encryption and ensured the safety and privacy of online experience by stating that law enforcement's right can only be implemented by a warrant. And hence privacy of the public will be protected by relevant authorities. The in-built oversight mechanisms of the *Assistance and Access Act 2018* and the required review from technical assessors will ensure the communications of Australians in general will not be jeopardized [7]. While in response to worried surveillance on everyday Australians from Australian Signals Directorate, Burgess [7] stated that ASD was not granted such power by the Act but a limited requesting assistance on cyber security matters only, which will not endanger public privacy.

With respect to one of the most popular concerns on mass surveillance that may be enabled by *Assistance and Access Act 2018*, and hence jeopardized public privacy and decreased public trust, the Department of Home Affair [8] responded that the Act does not provide such authorizations since interception capability and data retention capability are both prohibited under section 317ZGA of the Act.

For the past few decades, a variety of governments from worldwide have been making efforts to lobby more legislative powers in assistance with access to encrypted communications data intending to mitigate negative impacts of rapidly developed encryption technology on law enforcement's investigation capabilities. In United States, as part of the Clinton Administration program, the Clipper Chip was proposed but abandoned later on [4]. In a more recent case, Theresa May, current UK's prime minister, commented on various occasions that encryption should be banned [12], and has repeatedly called for crypto backdoors [13].

5. Conclusion

In conclusion, *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, though has sophisticated oversight mechanism and takes into consideration the most concerned systemic weaknesses security issue, its definition and guidance are vague and is likely not practical to achieve what the Act is designed for in practice. The potential overreach of the Act not only will impose great threats to system security as a whole, but also will breach the principle of privacy. Above implications have already affected Australian technology companies on global market. Moreover, the Five Countries governments have been long making efforts in promoting similar encryption access laws, and with Australia setting up a precedent, it is likely that the rest of Five Countries will follow suit.

References

[1] *Parliament of Australia (2018), Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, Parliament of Australia, Canberra.*

[2] *Bogle, A. (2019), Encryption laws developed after little consultation with Australian tech companies, FOI documents reveal, ABC.*

[3] *The Institute of Electrical and Electronics Engineers (2018), In support of strong encryption, issue paper, The Institute of Electrical and Electronics Engineers, New Jersey.*

[4] *Abelson, H., Anderson, R., Bellovin, S., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P.G., Rivest, R.L., Schiller, J.I., Schneier, B., Specter, M.A., & Weitzner, D.J. (2015). Keys under doormats. Communications of the ACM, 58(10), 24-26.*

[5] *European Union Agency for Network and Information Security (2016), ENISA's opinion paper on encryption, European Union Agency for Network and Information Security, Athens.*

[6] *Kopsias, A. (2019). National security and privacy: 'Going dark': The unprecedented government measures to access encrypted data. Law Society of NSW Journal, 52, 74-77.*

[7] *Burgess, M. (2018), Director-General ASD statement regarding the TOLA Act 2018, Australian Signals Directorate.*

DOI: 10.54254/2753-7048/53/20240056

[8] Department of Home Affair (2019), Myths about the Assistance and Access Act, Department of Home Affair, Canberra.
[9] Law Council of Australia (2018), Rushed encryption laws create risk of unintended consequences and overreach, Law Council of Australia, Canberra.
[10] Sarraf, S. (2018), Federal Govt releases proposed reform to access encrypted communications, CIO.
[11] Department of Home Affair (2018), Statement of Principles on Access to Evidence and Encryption, Department of Home Affair, Canberra.
[12] Revell, T. (2017), Theresa May's repeated calls to ban encryption still won't work, New Scientist.
[13] McCarthy, K. (2018), Here we go again... UK Prime Minister urges nerds to come up with magic crypto backdoors, The Register.