Commissioner brief: Encryption

Type: Commissioner brief

Purpose: Senate Estimates hearing, February 2018

For: The Australian Information Commissioner

Critical facts and key dates summary:

- At the Five Eyes conference in Ottawa on 26 June 2017 and at the G20 in Hamburg in early July 2017, Australia expressed support for adopting a common position on the legal obligations of technology companies to provide access to encrypted messages, to create consistency and facilitate the exchange of warrants seeking access to data from overseas counterparts.
- On 14 July 2017, the Attorney-General gave two media interviews outlining two options that the Government is considering to secure the cooperation of telecommunications and technology companies (such as internet service providers, Facebook, WhatsApp, Wickr and Apple) to access encrypted messages for use by law enforcement and intelligence agencies.
- Two options proposed were:
    1. A series of understandings or protocols that technology and telecommunications companies will enter into voluntarily, or
    2. Legislation, to be put before Parliament before the end of 2017,[1] that would oblige technology and telecommunications companies to provide access to encrypted messages.
- On 22 November 2017, the OAIC Section 47C - deliberative processes [redacted]
- The OAIC's *Guide to Securing Personal Information* identifies encryption as an important tool to securing information against attacks or in the event a device is lost. The OAIC may consider its use to be a reasonable step for an entity to take under APP11. The

[1] <http://pandora.nla.gov.au/pan/21248/20171220-1246/www.attorneygeneral.gov.au/transcripts/Pages/2017/ThirdQuarter/Interview-with-Kieran-Gilbert-SKY-News-14-july-2017.html>

Content Author:	Responsible Director:	Responsible Assistant Commissioner
Author's number:	Director's number:	Melanie Drayton

guide specifically asks entities to consider whether they should employ encryption of data in transit, for example data transferred over the Internet.

- APP 11 will apply to material communicated via a communications service that employs end to end encryption, such as WhatsApp or Wickr, to the extent that the material contains personal information.

Commissioner brief: Encryption

Background

- At the Five Eyes conference in Ottawa on 26 June 2017 and at the G20 in Hamburg in early July 2017, Australia expressed support for adopting a common position on the legal obligations of technology companies to provide access to encrypted messages, to create consistency and facilitate the exchange of warrants seeking access to data from overseas counterparts.[2]
- On 14 July 2017, the Attorney General gave two media interviews outlining options that the Government is considering to secure the cooperation of telecommunications and technology companies (such as internet service providers, Facebook, WhatsApp and Apple) to access encrypted messages for use by law enforcement and intelligence agencies.
- The Government is particularly concerned with preventing and investigating terrorism-related offence, as well as organised crime and paedophile networks.
- Two options that were proposed at the time:
    1. A series of understandings or protocols that technology and telecommunications companies will enter into voluntarily, or
    2. Legislation to be put before Parliament before the end of 2017 that will oblige technology and telecommunications companies to provide access to encrypted messages.
- On 22 November 2017, Section 47C - deliberative processes [redacted]

[2] See, for example, <https://www.lexology.com/library/detail.aspx?g=68063160-8924-4e97-89d5-a32014707adc>

Section 47C - deliberative processes

[redacted]

- Several issues were raised in the two interviews, as well as in media reports more generally:
  1. Resistance from companies – e.g. Apple's refusal to cooperate with requests to assist with accessing one of its phones during the 2015/16 San Bernardino, California terrorism investigation.
  2. How companies will be able to provide access without creating a "backdoor" into the encryption software or the device, as some encrypted communications are sent using end-to-end encryption.
     - Where encryption is not end-to-end, a message would be typically be sent to a company's servers, and then on to the recipient, but could potentially be accessed by the company while in transit.
     - Where end-to-end encryption is used, the company providing the service does not have the ability to decrypt communications.

- Some media reports[3] indicate that in these instances, the warrant would need to be issued to the sender or receiver of the communication, since these parties would be able to provide access to the unencrypted text.
- The current lack of detail as to how access will be provided is a concern for technology companies such as Apple, with representatives from that company recently meeting with the Attorney General and senior staff from the Prime Minister's office to outline Apple's position that any legislation should neither prohibit companies from using encryption on their devices, nor require companies to provide decryption keys.[4]

3. If "backdoor" access is required, then the flaws written into the software or system can create their own security concerns if exploited by hackers.
4. Even if cooperation from major companies could be secured, users may create or adapt their own encryption applications, or rely on services in other jurisdictions.
5. Exacerbate community concerns regarding mass surveillance of everyday private communications.

Rapid increase in the use of encryption

- There has been a significant increase in the use of encrypted communications in the last few years.
  - In 2013, approximately 3% of ASIO's priority investigations involved attempts to access encrypted information, which has increased to more than 50% in 2017.

Encryption

- When a communication is encrypted, it is scrambled to make it unreadable except to the person (or device) that has a "key" to unlock it.
- Messages sent using "end-to-end" encryption typically can only be read by the sender and receiver, who hold the requisite keys to unscramble the message.
- The telecommunications provider and the messaging service (such as WhatsApp) do not hold the right keys to decrypt the message whilst it is in transit, and therefore cannot intercept the content of communication and provide it to law enforcement or security agencies in the same way that they can currently intercept non-encrypted communications.

UK and NZ measures

[3] <http://www.smh.com.au/federal-politics/political-news/how-the-turnbull-government-plans-to-access-encrypted-messages-20170609-gwoge0.html>
[4] <http://www.smh.com.au/federal-politics/political-news/apple-flies-in-top-executives-to-lobby-turnbull-government-on-encryption-laws-20170719-gxebvn.html>

- In 2013, NZ introduced the *Telecommunications (Interception Capability and Security) Act 2013*
  - This Act requires a network operator to decrypt an encrypted communication if it has provided the encryption.
  - However, there is no obligation to decrypt the communication if it was encrypted by another entity.
- In 2016, the UK introduced the *Investigatory Powers Act 2016*
  - This Act requires regulated entities to do everything reasonable within their power to enable law enforcement agencies to inspect encrypted messages or to inspect devices.
  - The UK has recently released draft *Investigatory Powers (Technical Capability) Regulations 2017,* issued under the *Investigatory Powers Act 2016*. As part of the draft regulations, "technical capability notices" may be issued to a telecommunications operator to ensure that it has the capability to provide assistance in giving timely effect to a warrant requiring access to an encrypted communication.
  - There is debate in the UK as to whether the legislation and regulations are effectively outlawing end-to-end encryption or requiring companies to create backdoors into their devices or software.