Australian National University

National Security College

POLICY OPTIONS PAPER

No 8, April 2018

Defining thresholds in law – sophisticated decryption and law enforcement

Michelle Mosey and Adam Henschke

Key points

- Encryption technologies have fundamentally changed the way people transmit data, reducing the capacity of law enforcement and intelligence agencies to access information.
- Relying on the private sector to provide agencies with plain text information is no longer productive, yet legislation and frameworks have not caught up.
- Undermining the integrity and security of encryption by mandating the creation of access points in software creates an unacceptable risk to all information security.
- Due to the incompatibility of current technologies and legislation, Australian law enforcement and intelligence agencies may need to operate in a grey area which lacks legislative direction. Regardless of their professionalism, this introduces risks for information security and human rights.
- The fundamental legal and moral approaches to collection of encrypted information need to be reconsidered to balance community trust and public confidence with the ability to deploy sophisticated decryption technologies.

Policy recommendations

- Governments should transparently review the principles behind collection of encrypted information to ensure community trust and ethics are balanced with agency capability needs.
- Legal changes are required to codify the powers and thresholds under which law enforcement and intelligence agencies can circumvent strongly encrypted devices.
- Relevant legislated oversight mechanisms should be put in place, modelled upon currently applicable intelligence oversight.

Decryption in law enforcement

Strong encryption provides an important function for the protection of information security and integrity, which is a net benefit to our society and economy. It is increasingly being adopted by the public and technology providers. This however does not reduce the need for law enforcement and intelligence agencies to access and collect information relevant to national and domestic security.

To enable agencies to fulfil their responsibilities, they will require legislated powers that determine thresholds at which particularly sophisticated decryption and access tools may be applied for collection against domestic intelligence targets. Failure to legislate such powers may expose law enforcement and intelligence agencies to breaches of human rights and democratic norms. More importantly, it may damage public trust in Australian law enforcement and intelligence agencies, as well as undermine the supremacy of law in the investigation of criminal activities.

Recently in comparable foreign jurisdictions, we have seen domestically focused law enforcement agencies requesting 'backdoors' be built into encrypted communication devices and applications, for use in particular national security emergencies. However, such backdoors reduce the security and integrity of our information collectively and over the long term, as it is not possible to ensure they are used only by those agencies. The security of our society relies upon the security of our information. We do not become more secure by increasing its vulnerability.

New communication technologies

Strong encryption refers to those methods considered unbreakable by the NSA and FBI. In 2000, the United States Government removed restrictions on the sale of strong encryption to allow its use for online trade. Use of encryption has expanded rapidly since then. In particular, there has been a strong trend towards the adoption of end-to-end and other powerful encryption technologies in online messaging applications, which constitute a growing share of online communication.

Encryption of communications provides significant challenges for law enforcement and intelligence agencies, particularly given the law has not kept pace with technology. In Australia, the legal basis for information collection remains in the *Telecommunication Intercept and Access Act 1979* and the *Intelligence Services Act 2001* – both were designed before information was routinely encrypted.

For example, end-to-end encryption is designed so that no third party, including the service provider, has knowledge of the private encryption key required to access the plain text communication. Communication service providers are unable to decrypt the message and provide its plain text content to domestic law enforcement agencies under warrant as was the case under existing legislation. Only the meta-data, or the 'digital exhaust' created by the transmission can be accessed.

A similar challenge is full disk encryption. If iOS and Android devices adopted full disk encryption, the Centre for Strategic and International Studies estimates 99 percent of the world's smartphones could become inaccessible to law enforcement.[1]

Despite these challenges, strong encryption has many legitimate uses, including protecting private communication, and securing essential government and commercial activities. However, it is also very often used to hide criminal and terrorist activities. In response, government agencies are seeking to decrypt devices, however on the basis of unclear legal guidelines and outdated legislation.

A court order to endanger global information systems

A recent legal case in the US highlighted the issues at play. In *United States District Court for the Central District of California v. Apple Inc.*, Apple was ordered to create software enabling the FBI to bypass the security encryption of an iPhone owned by Syed Farook, one of the San Bernardino shooters. Apple rejected this order due to the broader consequences of creating such software, including repercussions for general information security and the reputational harm if consumers became aware that Apple could break into its customers' phones.

"Apple did not oppose the FBI's right to a legal search of the phone with a warrant: instead, the company objected to the court forcing it to reverse engineer its encryption",[2] creating an access point in all device software and possibly jeopardising broader information security.

In a world where the question is not *if* they will be hacked, but *when* they will be hacked, individuals place a high value on information integrity, security, secrecy and privacy. These require encryption. Moreover, the modern digital economy relies on sharing digital information and being able to trust and ensure the integrity of all information.

Most dangerously, mandating in law the creation of access points will threaten all information security and the integrity of all devices. A purpose built backdoor for law enforcement is a backdoor for all.

A dangerous legal precedent?

After Apple refused to heed the court's order to create an access point, the FBI was approached by a foreign private company which cracked the phone's encryption. The FBI engaged the company without a clear legal basis.

This precedent raises significant risks, given the amount of money the FBI was reported to have paid (between $900,000 and $1.3 million). It may inadvertently create a competitive private-sector incentive for firms to compromise the encryption used by millions of devices around the world.

The recent announcement of the GrayKey 'unlock tool', recently advertised as capable of performing up to 3000 iPhone password unlocks for $15,000, is the first high profile example of a 'hack for sale' product. Private companies with this capability will continue to commercialise it and make decryption more widely available, undermining the information security of all devices.

No information was provided publicly by the FBI outlining its decision-making process, nor the legal basis upon which it engaged the assistance of a foreign private-sector entity. There are legal questions over evidentiary standards while using unlegislated decryption tools produced by the private-sector. Also, when law enforcement agencies appear to be operating outside the law, public confidence and trust in those agencies rapidly erodes.

Both the court order and the FBI's solution raise a further social and legal concern. "By demanding that companies facilitate the intrusion into the private sphere, law enforcement indirectly outsources a key policing function to private corporations", a previously state-monopolised function.[3]

Failure to legislate

Domestic law enforcement and intelligence agencies have always required specialised capabilities to access information which would otherwise be inaccessible. Failure to legislate appropriate powers in relation to cyber capabilities has placed government agencies at risk, possibly undermining oversight and reducing public confidence.

For example, private-sector-developed malware and spyware has been used domestically by German authorities since 2011, despite the lack of explicit enabling legislation. As a result, security agencies have been accused of overreach.

In 2016, the German Interior Ministry confirmed that it had "approved the usage of Trojans to monitor suspected citizens". Similar to traditional telecommunication intercepts as codified in law, "in order to use the malware, government officials will have to get a court order, allowing authorities to hack into a citizen's system".[4]

While this transparency and due process is welcomed and encouraging, such powers should be defined in legislation and exercised under strict oversight in accordance with other similarly invasive intelligence powers.

The Australian context

As currently enacted, Australian laws do not set out a process for yielding intelligence from these technologies. We need a more solid legal basis to ensure accountability and public confidence.

For example, as a result of technological changes, the targeted use of offensive and defensive cyber capabilities against foreign targets – under "stringent legal oversight

and consistent with our obligations under international law" – has become a part of Australian Government policy.[5] It is not clear to the public what this oversight is, how it works and, importantly, how this may impact their personal privacy and security.

The *Telecommunication (Intercept and Access) Amendment (Data Retention) Act 2015* is a step in the right direction. It acknowledges the challenges faced by law enforcement due to technological advances and the increasing obsolescence of technologies for which current legislation was designed. The explanatory documents to the Act outline thresholds pertaining to the use of particular powers by 'enforcement agencies' to ensure oversight, proportionality and adherence to human rights, while mandating data retention, intercept and access powers. The Act also explicitly excludes content from being retained.

The need for law and more

The changing nature of encryption technologies will require legislated powers to determine thresholds at which particularly sophisticated decryption and access tools may be applied for law enforcement efforts against Australian targets.

If enacted into legislation, the use of active tools and decryption capabilities could consider and develop thresholds for particular categories of criminal offences, based upon their severity and impact. This would determine the agencies capable of using such powers and the sort of intrusive or active capabilities they may deploy in order to access devices in connection to specific criminal offences committed in Australia. Collection processes must adhere to relevant standards of evidence to facilitate a prosecution in a manner consistent with the ideals of human rights, transparency and proportionality.

Legislating will not address the main concern that lies at the heart of this issue – privacy for users. While the question of how much privacy needs to be relinquished to protect the public remains, we cannot expect the public to trust agencies to respect their privacy with no transparency or apparent accountability.

Endnotes

1 J Lewis, D Zheng & W Carter, *The Effect of Encryption on Lawful Access to Communications and Data*, CSIS, 2017.

2 A Glenster, 'Decrypting Apple: Making Technology Companies the Referees of Law Enforcement on Privacy', Jolt Digest, 2017.

3 Ibid.

4 http://www.dw.com/en/german-spyware-scandal-expands-to-political-legal-circles/a-15475258

5 https://www.pm.gov.au/media/2017-06-30/offensive-cyber-capability-fight-cyber-criminals

About this publication

This series of National Security College Policy Options Papers offers short, evidence-based and forward-looking insights for policy-makers on topical security, foreign affairs and geostrategic issues facing Australia domestically, in the Indo-Pacific region and globally. We seek contributions from and collaborations with qualified researchers and experts in these fields.

T +61 2 6125 1219
E national.security.college@anu.edu.au
W nsc.anu.edu.au

@NSC_ANU
National Security College

CRICOS Provider #00120C

About the authors

Michelle Mosey is the former Senior Adviser for Cyber Policy at the ANU National Security College.

Dr Adam Henschke is Senior Lecturer and Graduate Convenor at the ANU National Security College.

The NSC wishes to thank Mr Michael York for his research in support of this paper.

The National Security College is a joint initiative of the Commonwealth Government and The Australian National University

MO_NSC180905