accessnow

THE ROLE OF ENCRYPTION IN AUSTRALIA

A MEMORANDUM

JANUARY 2018

The authors of this document are Lizzie O'Shea and Elise Thomas, with support from Access Now and assistance by Nathan White, Amie Stepanovich, and the Access Now Policy Team.

Access Now defends and extends the digital rights of users at risk around the world. By combining innovative policy, global advocacy, and direct technical support, we fight for open and secure communications for all.

For more information, visit https://www.accessnow.org

EXECUTIVE SUMMARY

- Encryption is essential to Australia's modern digital society, economy, and cyber security, and it is only effective if it is strong and robust.
- Strong encryption serves Australia's national interests by protecting governments, communities, and the economy from criminal, terrorist, and state-sponsored attacks.
- Encryption will only become more important for protecting Australian interests as technology advances in the coming decades.
- The government is proposing to weaken encryption in the name of fighting terrorism, however this policy would create more security risks than it addresses.
- There are other policy options for dealing with terrorist use of digital technology that are more urgent and effective than weakening encryption.

BACKGROUND TO THE CURRENT DEBATE ABOUT ENCRYPTION

Encryption is a method for ensuring communications between two parties remain private from everyone else, including the carrier. Even if an encrypted communication is intercepted by a third party, it cannot be read by anyone except the people who are authorised to decrypt it. Encryption is a foundational tool for the proper functioning of the digital society and economy, and is used in a wide range of settings, including banking, public service delivery, and communications systems.

At various times governments have attempted to regulate encryption, with little success. Most recently in the UK, the government has introduced the Investigatory Powers Act, which requires technology companies to assist the government to decrypt messages where technically feasible. It is unclear what this provision means in practice for companies and individuals that rely on encryption. The act is still being implemented, so it has not yet been possible to observe how it will be used.

Prime Minister Malcolm Turnbull has stated that his government wants to introduce a method for intercepting and reading encrypted messages. In July 2017, he discussed giving law enforcement this power for the purposes of keeping the public safe from terrorism. In that same press conference, former-Attorney General George Brandis argued that the government's surveillance powers needed to be brought up to date by requiring that technology companies cooperate with law enforcement. Attorney General Brandis indicated that this initiative is part of Australia's participation in the Five Eyes, and confirmed the government's commitment to intelligence sharing with these partners.

It is not clear how the government plans to implement these changes in law. This uncertainty suggests that the government does not appreciate the complexity of the issues involved. Approaches proposed or used in other countries include outright prohibitions on encryption, escrow of encryption keys, or limitations on the strength of encryption. Each of these has been demonstrated to have serious risks. Two of the most commonly discussed options in Australia have been to require technology companies to build a 'backdoor' to allow direct government access, or, conversely, to obligate companies to build into systems the capacity to decrypt the messages and then hand the information over to the government. Attorney General Brandis has indicated that mandating a backdoor is not the government's plan, however he has also stated in June 2017 that 'if there are encryption keys then those encryption keys have to be put at the disposal of authorities.'

The reactions from experts and commentators have highlighted deep problems with the government's general plan. Academics have outlined the flaws from an engineering perspective. 'Decrypting terrorists' communications without undermining the security of everyone else sounds great,' wrote academics from the University of Melbourne, 'but this is not an engineering plan and every known attempt has failed.' Built-in weaknesses in encryption systems are not features that can be exploited only by the government; they can also be used by criminals and foreign enemies. Information about any backdoor will be highly valuable, and a honeypot for hackers, making it hard to keep safe. In July 2017, private health insurer Bupa notified tens of thousands of their customers that their private information had been leaked by a rogue employee – demonstrating the immense security risks facing institutions charged with protecting data. Journalists have also pointed out that the proposal is unlikely to be effective for its intended purpose: terrorists can, and likely will, move to other communication channels that have strong encryption. Civil society organisations have argued that police already have significant powers to investigate terrorism and this proposed extension of surveillance capabilities has not been justified.

The government's Digital Economy Strategy, Cyber Security Strategy, and International Cyber Engagement Strategy each confirm the importance of digital technologies and cyber security for Australia in the years ahead. Encryption is a crucial element of all cyber security strategies. The purpose of this paper is to demonstrate that encryption is essential to the digital society, and encryption is only effective if it is robust. A system of encryption with a back door is like a chain with a fatally weak link – the strength of the entire system is compromised and it is only a matter of time before it breaks, jeopardising the safety of everyone who relies on it. This risk has profound implications for systems and infrastructure that we rely on for our daily lives.

ENCRYPTION TODAY

Encryption plays a major role across many important areas of Australian life, including national security interests, the economy, and protecting the community, individuals, service providers, and the private sector from crime and other risks.

Encryption is essential to many government activities

NATIONAL SECURITY

The integration of digital technology into almost all government practices makes cyber security an essential part of national security. The Australian Cyber Security Centre (ACSC) notes that in 2017, all federal and state government networks were 'regularly targeted' by actors ranging from cybercriminals to state-sponsored adversaries. Many states in our region are rapidly developing their cyber capabilities for both defensive and offensive purposes. The ACSC responded to 671 cyber security incidents impacting government between 1 July 2016 and 30 June 2016. Encryption offers an essential line of defence against such attacks.

GOVERNMENT DATASETS

Large government datasets, such as the MyGov system, are highly tempting targets for malicious state actors and cyber criminals. Earlier in 2017 it was discovered that a hacker had infiltrated and stolen data from Medicare, and was selling Australians' personal information to the highest bidder. Incidents such as this not only put individuals at risk of crimes such as identity fraud, they also damage the public's trust in the government to keep their data safe online. As various government bodies continue to improve their digital services and consolidate datasets, it is crucially important to protect these assets using cyber security best practices, of which strong encryption is one.

CONTRACTORS AND SERVICE PROVIDERS

The range of potential targets is not limited to systems directly operated by government. The ACSC has said that as government defences improve, adversaries are likely to look for softer targets to attack or disrupt, including contractors and service providers. An attack on IT company Deloitte may have allowed hackers to steal emails from multiple US government departments. It has also been recently revealed that Australian government contractors have been successfully hacked and had large amounts of data stolen. Defence and intelligence agencies, as well as law enforcement, are especially likely to be targeted by highly sophisticated and capable adversaries. Defending information systems and deterring hackers requires strong encryption at a range of levels, from major government databases to personal devices of individual contractors.

ESSENTIAL INFRASTRUCTURE

Operators of public infrastructure are also vulnerable. In late 2016, a ransomware attack on the San Francisco metro shut the ticketing system down for two days. A minor computer glitch which stopped all trains across Melbourne in July 2017, stranding thousands of passengers, demonstrated how disruptive interference with these systems could be. A deliberate and sustained attack on major public transport systems, or the electricity grid as has happened in Ukraine, could cause chaos in Australian cities. These infrastructure systems are put at risk if they are not protected by strong encryption.

Encryption is the lynchpin of the modern financial system

BANKING

The vast majority of the world's money now exists only in a digital format. Security is the key promise that banks make to customers who deposit money with them. Banks are obvious targets for cyber criminals, and 'bank grade security' has become synonymous with best practice in this field. Nonetheless, banks around the world have fallen victim to hackers, with over a billion dollars stolen in some cases. The increasing sophistication and ambition of these modern bank robbers should serve as a warning about the importance of supporting banks and financial service providers to implement the strongest possible cyber defences, including strong encryption.

CARD PAYMENTS

Australians now make the majority of their purchases digitally (using debit and credit cards) rather than paying in cash. Encryption is central to card payments both online and through point-of-sale machines such as EFTPOS, because it protects sensitive customer data like PINs from being stolen or intercepted. The Payment Card Industry Security Standards Council, which includes companies like Visa and MasterCard, requires anyone processing card transactions to use strong encryption under the Data Security Standards. These companies take their responsibility to encrypt and protect customer data extremely seriously. Accommodating a government policy which undermines the strength of their encryption would present a very challenging task for companies in the payment card industry and the businesses that rely on it.

DIGITAL COMMERCE

The government's Digital Economy Strategy estimates that digital technologies could add up to $250 billion to Australia's GDP by 2025. In order for these benefits to be realised, it is important that the technologies which online businesses rely on are secure and align with global standards. Poor cyber security practices like weak encryption leave businesses vulnerable to costly criminal attacks and stifle entrepreneurship in Australia's digital economy.

Encryption protects communications and data sharing systems

INDIVIDUALS

Data breaches, which lead to theft and exposure of the data about individuals, can have significant personal, professional, and legal ramifications. The hack of 'infidelity site' Ashley Madison is just one example in which leaked data impacted personal relationships, damaged professional reputations, and exposed individuals to risks such as identity theft. Consumers rightfully expect that their personal data will be stored securely, including through the use of strong encryption. Encryption protects messages between individuals where they would have a reasonable expectation of privacy, but the issue is much larger than personal communications. For example, the recent leak from credit reporting agency Equifax has exposed at least 143 million people to the risk of identity theft and other crimes. Consumers have a reasonable expectation that messaging platforms and storage systems for personal data will be kept secure, including through the use of strong encryption.

CRITICAL SERVICES

Critically important service providers such as hospitals rely on complex information technology systems for sharing data about patients and services. They are regular targets of cybercriminals. The WannaCry attack in May 2017 hit 16 UK hospitals, preventing them from accessing their patient data system and leading to cancelled surgeries, diversion of ambulances, and widespread disruption of medical services. Protecting the ongoing operation of hospitals and other vital services is a top priority and demands the strongest defences technology can provide.

PRIVATE SECTOR

Private sector professionals and businesses with access to sensitive or commercially valuable information are prime targets for commercial espionage by both local and international hackers. Small businesses are also vulnerable, and it has been reported that 59% of Australian businesses recorded cyber security breaches in 2016. A report by IBM and the Ponemon Institute found that the average total cost to an Australian business which suffered a data breach in 2017 was $2.51 million. The report found that malicious attacks are the most common cause of data breaches. Motivations for attacks on the Australian private sector range from international espionage to intellectual property theft, according to former head of the U.S. CIA Bill Hayden. Supporting businesses and ensuring that Australia's private sector remains globally competitive must include allowing access to the best possible defences against criminal attacks.

ENCRYPTION TOMORROW

The rapid pace of technological advancement means that laws made today – which may remain in force for years or decades to come – must consider not only the present situation but also the foreseeable future. As technology becomes ever more deeply embedded into Australia's economy, society, and national security, encryption will only become more critical to the protection of Australian interests.

Encryption is needed to create a modern, competitive economy

Australian companies must be able to protect themselves against crime and, in turn, attract international investment. This requires that businesses use the highest possible standards in cybersecurity. New financial technologies such as the blockchain and cryptocurrencies as well as the growth in other technology industries will only increase the need for encryption. If development in encryption is limited, companies deploying these technologies will likely look elsewhere rather than invest in Australia. Undermining encryption would put Australia at a competitive disadvantage against other nations as their cyber defences continue to improve.

Encryption is needed to prevent crime and enable law enforcement

The frequency, seriousness, and sophistication of cybercrime will grow in the coming decades. Strong encryption is necessary to help keep the public safe from both new kinds of crime, and traditional crimes aided by new technology. It will also be needed by law enforcement and intelligence agencies to defend themselves and the public against criminal, terrorist, or state-sponsored adversaries. As more data are collected and stored by police, security, and intelligence agencies, the digital assets and networks of these agencies will increasingly come under threat from outside attackers. Protecting the integrity of policing and intelligence systems is crucially important for the safety of all Australians.

Encryption is needed for a safe, prosperous modern society

The Internet of Things, smart cities, autonomous vehicles, and a host of other exciting new technologies will play a major role in Australian life over the coming decades. In order for Australians to enjoy the benefits of these new technologies, it is important to also guard against the risks. Other countries, like China, are responding to modern challenges by investing in quantum cryptography. Australians deserve and expect protections of the highest international standard to keep our communities safe in the years to come.

SOLVING PROBLEMS WITHOUT UNDERMINING SECURITY

The Turnbull government has expressed concern about terrorists using encryption to evade surveillance, but this concern misses some important considerations. The case for weakening encryption has not been made out, especially in a context in which so many everyday digital activities would be put at risk.

Weakening encryption will create more vulnerabilities that can be exploited by criminals.

By aiming to weaken encryption, the government will create more national security problems than it addresses. The government has not made public its plans for storing and protecting the information that it will gather as part of building and using a backdoor or other tool to bypass or limit encryption. Such valuable information will be enticing to criminals. Consider that recently the US Securities and Exchange Commission disclosed that its central database was hacked, with the information possibly used for insider trading purposes. The government has not demonstrated that it is prepared for similar such assaults.

Law enforcement and intelligence service already have immense powers and capacity for surveillance.

This includes a mass data retention regime that is very similar to a proposal rejected by the European Court of Justice as being unnecessary and disproportionate. This also includes powers to compel the production of private encryption keys and passwords, as well as powers to access computer infrastructure and endpoints. The problem is not that law enforcement and intelligence agencies lack surveillance powers.

There are clearly other, much larger problems that are being encountered by law enforcement tackling terrorism than access to encrypted communications.

Criminal investigations are currently being delayed by months and even years as police struggle to find the right expertise for examining information stored on devices. Arguably, the more urgent priority is training of digital forensic and cyber-crime specialists, and supporting them to work in law enforcement.

The government should focus on the reform of Mutual Legal Assistance Treaties (MLATs) instead of weakening encryption to improve law enforcement process

MLATs between Australia and other countries include arrangements for information sharing for law enforcement purposes. These processes tend to be slow, opaque, and inefficient. Reform of MLATs is an urgent priority to ensure that intelligence is shared in a timely and effective manner. It would allow intelligence agencies to make better use of evidence they already have, rather than encourage them to seek access to evidence they do not yet have (like encrypted messages). The reform of MLATs ought to be a focus of the government.

The government's job is to develop policies that protect national security without endangering public safety and economic interests. The focus on weakening encryption does not meet these requirements.

CONCLUSION

Strong encryption protects Australian interests and keeps ordinary Australians safe. It serves the interests of anybody who uses internet banking, shops online, relies on modern public services, and expects their personal information to be kept private. Weakening encryption creates risks to the safety of everyone, as well as businesses and public service providers. It also sets Australia back relative to our global competitors. Policies that undermine strong encryption create more problems than they solve, and it is critical that legislators and decision makers consider the consequences before it is too late.