By Simon Frew and Tom Randle

Introduction

Pirate Party Australia would like to thank the Parliamentary Joint Committee on Law Enforcement for the opportunity to contribute to the debate around the impact of new and emerging information and communications technology (ICT) and its relationship to law enforcement.

Our submission will primarily focus on the risks posed to society by trying to regulate encryption, something that we believe will damage the safety and functionality of the Internet, a tool that has become vital to the entire population in recent years. As such, we will not address all of the terms of reference explicitly, but provide general commentary on developments in ICT and ways of addressing arising issues faced by Law Enforcement Agencies (LEAs).

It is the view of Pirate Party Australia that mandating access to encrypted communications is unnecessary for a number of fundamental reasons, including that there are many other ways available to LEAs for monitoring the activities of alleged criminals. Any legislative attempt to regulate encryption will continue the erosion of Australians' civil liberties, it will be unworkable and is a risk to the future development of the Australian economy. The primary fundamental reason governments should not attempt to use the force of law to require access to encrypted information is that there will be circumstances where a person required by LEAs to assist in gaining access to supposed encrypted information will be physically unable to comply, as the laws of mathematics in this universe make complying with such requests literally impossible.

About Pirate Party Australia

Pirate Party Australia is a political party based around the core tenets of freedom of information and culture, civil and digital liberties, privacy and anonymity, and government transparency. It formed in 2008, and is part of an international movement that began in Sweden in 2006. Pirate Parties have been elected to all levels of government worldwide.

Law enforcement in the online environment

With the proliferation of the Internet, LEAs have had to adapt to the new technologies, as have almost every sector of society. Eager to appear tough on crime and terrorism, state and federal governments have legislated a raft of new powers, including warrantless mass surveillance under the **Telecommunications (Interception and Access) Amendment** (Data Retention) Act 2015 which, in our opinion, has shifted the balance between privacy for the individual and access to information by the state, firmly in favour of the state. The information available under the data retention regime amounts to warrantless monitoring and location tracking of the vast majority of the population, with historical data being searched 332,639 times during the 2015-16 reporting period.[1] The extension of law enforcement capabilities has continued unabated since 2001, with over 50 legislative changes, granting more powers to security services and eroding Australians' civil liberties.[2]

The information made available through metadata is quite revealing. ABC journalist Will Ockenden published his metadata in 2015 and it revealed a lot about his movements, his contacts and associations.[3] Last year, the Australian Federal police (AFP) had illegally searched a journalist's metadata, beaching their privacy with no penalty, something that the journalist was not made aware of, despite the seriousness of the privacy breach.[4] Such detailed information about the personal lives of citizens should require legal oversight in the form of warrants at the very least.

Civil liberties issues aside, there are a wide range of methods that LEAs can use to access the communications of persons of interest that do not require encryption to be weakened.

The Berkman Centre for Internet and Society at Harvard University eloquently debunks the "going dark" myth in it's paper Don't Panic: Making sense of the Going Dark Debate.[5] It also demonstrates a range of ways in which communications can be monitored without damaging the security available to the public. From the paper:

- Short of a form of government intervention in technology that appears contemplated by no one outside of the most despotic regimes, communication channels resistant to

---

1 https://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/Telecommunications-Interception-and-Access-Act-1979-Annual-Report-15-16.pdf Pg 49

2 https://www.theguardian.com/australia-news/ng-interactive/2015/oct/19/all-of-australias-national-security-changes-since-911-in-a-timeline

3 http://www.abc.net.au/news/2015-08-24/metadata-what-you-found-will-ockenden/6703626

4 http://www.abc.net.au/news/2017-04-28/afp-officer-accessed-journalists-call-records-in-metadata-breach/8480804

5 https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf Pg 2

> surveillance will always exist. This is especially true given the generative nature of the modern Internet, in which new services and software can be made available without centralized vetting. However, the question we explore is the significance of this lack of access to communications for legitimate government interests. We argue that communications in the future will neither be eclipsed into darkness nor illuminated without shadow. Market forces and commercial interests will likely limit the circumstances in which companies will offer encryption that obscures user data from the companies themselves, and the trajectory of technological development points to a future abundant in unencrypted data, some of which can fill gaps left by the very communication channels law enforcement fears will “go dark” and beyond reach.

The raft of new powers that have been granted to LEAs since 9/11 more than make up for any loss of access to the contents of encrypted communications. Metadata is unencrypted and legally accessible as it is, and as demonstrated above, provides access to a wide array of personal data from individuals including location data and who they make contact with.

Ubiquitous end to end encryption is against the business interests of companies for many of their current services. Companies like Google and Facebook keep detailed personal information on their users for advertising and commercial purposes. The proliferation of mobile hand held devices such as smartphones and tablets has led to a huge expansion of data being stored in central locations through cloud storage. Providing end to end encryption actually damages their business models. This data is already available to LEAs through normal warrant processes.

The Internet of Things, small devices that rely on computing to function and connect to the Internet, often have diabolically weak security. Society funds and resources LEAs in order to provide everyone with a reasonable expectation of safety in our offline and online lives. Governments must therefore make a choice regarding how flaws and weaknesses discovered or known by government agencies in technology is handled and all governments should be upfront and honest about the choice they make. The current trend in western democracies has been to empower LEAs and security agencies through vague legislation to exploit vulnerabilities in devices and software for surveillance and data exfiltration. But this necessarily means that the entire Australian population is left vulnerable. Pirate Party Australia recommends legislators prohibit LEAs and security agencies from hoarding vulnerabilities, and instead require the responsible disclosure of all vulnerabilities known by government agencies in the interests of public safety.

The need for unbreakable encryption

Online communications regularly carry information that people expect to be kept safe. The most obvious example of this is private financial information for online purchases, which is becoming a major part of the financial life of most Australians. The need for encryption is also obvious when considering other private information regularly shared online, such as passwords, medical

information, financial records etc.. All of this highly sensitive information is (or should be) currently protected by strong encryption.

Current day end to end encryption generally works by encoding messages with algorithms that are encoded with public and private keys. Each end of the communication requires a public key, which is used to scramble the message for the recipient and a private key which is used by the recipient to decode the encrypted message. Successful attempts to intercept the message in transit would just show the scrambled message. The more secure communications systems in use today generate the public and private keys anew with each communication, ensuring that if the private keys are somehow revealed they will be of no use on future communications. Any attempt to create a way for LEAs to decrypt communications creates a target which criminals and nation states will try to exploit. It is impossible at a technical level to create a safe way to give one group access to communications that cannot be exploited by other groups with more nefarious objectives. In *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications* a large number of prominent computer security experts came to the conclusion.[6]:

- This report's analysis of law enforcement demands for exceptional access to private communications and data shows that such access will open doors through which criminals and malicious nation-states can attack the very individuals law enforcement seeks to defend. The costs would be substantial, the damage to innovation severe, and the consequences to economic growth difficult to predict. The costs to developed countries' soft power and to our moral authority would also be considerable. Policy-makers need to be clear-eyed in evaluating the likely costs and benefits.

Computer systems already suffer from vulnerabilities that can have serious consequences for personal data, financial systems and infrastructure. The authors of Under Doormats demonstrate this through highlighting prominent security favours in the months before the papers' publication:

- The December 2014 North Korean cyber attacks against Sony, the first such by a nation-state, resulted in large headlines. But the 2011 theft from RSA/EMC of the seed keys — initial keys used to generate other keys — in hardware tokens used to provide two-factor authentication, and the recent theft of personnel records from the US Office of Personnel Management are far more serious issues. The former undermined the technical infrastructure for secure systems, while the latter, by providing outsiders with personal information of government users, creates leverage for many years to come for potential insider attacks, undermining the social infrastructure needed to support secure governmental systems — including any future system for exceptional access. And while attacks against critical infrastructure have not been significant, the potential to do so has

[6] https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf pp24-25

been demonstrated in test cases and in an actual attack on German steel mill that caused significant damage to a blast furnace.

- As exceptional access puts the security of Internet infrastructure at risk, the effects will be felt every bit as much by government agencies as by the private sector. Because of cost and Silicon Valley's speed of innovation, beginning in the mid-1990s, the US government moved to a commercial off the shelf (COTS) strategy for information technology equipment, including communications devices. In 2002, Information Assurance Technical Director Richard George told a Black Hat audience that "NSA has a COTS strategy, which is: when COTS products exist with the needed capabilities, we will encourage their use whenever and wherever appropriate... ". Such a COTS solution makes sense, of course, only if the private sector technologies the government uses are secure.

- Communications technologies designed to comply with government requirements for backdoors for legal access have turned out to be insecure. For ten months in 2004 and 2005, 100 senior members of the Greek government (including the Prime Minister, the head of the Ministry of National Defense and the head of the Ministry of Justice) were wiretapped by unknown parties through lawful access built into a telephone switch owned by Vodafone Greece. In 2010 an IBM researcher observed that a Cisco architecture for enabling lawful interception in IP networks was insecure. This architecture had been public for several years, and insecure versions had been implemented by several carriers in Europe. And when the NSA examined telephone switches built to comply with government-mandated access for wiretapping, it discovered security problems with all the switches submitted for testing. Embedding exceptional access requirements into communications technology will ensure even more such problems, putting not only private-sector systems, but government ones, at risk.[7]

It is important to highlight that IT security is an ongoing concern. The recent exposure of the Meltdown and Spectre vulnerabilities in virtually every computer chip built in the last 20 years is a catastrophic reminder that even systems that are believed to be secure can be hacked and data on the systems exposed. Simply put, the Meltdown and Spectre vulnerabilities work by exploiting processes built in at the hardware level of computer chips originally intended as a feature to speed up chip operations through predictive processing, where chips start processing multiple options of an operation before a decision has actually been made, and through caching, where data is stored on chips for rapid access when required. These vulnerabilities enable those using the now revealed exploits to uncover almost any private data in the memory of any computer system, data such as passwords and credit card numbers.[8] Whilst the companies responsible for producing the chips are rapidly working to help patch them at a software level,

[7] Ibid pp 9-10

[8] https://www.csoonline.com/article/3247868/vulnerabilities/spectre-and-meltdown-explained-what-they-are-how-they-work-whats-at-risk.html

the fix will actually result in a world wide slow down of computer processing power in general. These latest incidents highlight the precarious nature of computer security even before deliberate vulnerabilities or backdoors are required by governments to be built in.

Strong encryption is a driving force behind financial innovations referred to collectively as blockchain technologies, more popularly known as cryptocurrencies. Cryptocurrencies have been in the headlines a lot recently with large price fluctuations and a growing acceptance in financial markets. Most recently Goldman Sachs has provided cautious support for cryptocurrencies, especially in countries with unstable currencies.[9] The ASX have also begun work on its own blockchain technology to keep a distributed ledger of trades, making trading faster, cheaper and more reliable.[10] Blockchain technologies also offer ways to manage contracts and legal agreements[11], managing rights for advertising and royalties for intellectual property[12] and to improve participation in politics through voting systems.[1314] Blockchain technologies are secure precisely because they are designed with unbreakable encryption.

Risks of mandating access to encrypted communications

The most obvious risks to mandating backdoors to encryption is the direct risk to user security. When forced to deploy weakened security systems, in an already insecure environment the risks of hacks will increase significantly because the products are less secure by design. According to the Australian Federal Police, the Attorney-General's office estimates that the cost of identity theft on the Australian economy is estimated at 1.6 billion dollars a year.[15] This will inevitably go up significantly if security is weakened.

The UK's Snoopers Charter, a similar attempt to mandate backdoors to encryption has seen a number of technology companies move out of the country in order to be able to protect their products security from being weakened through legislation.[16] A similar exodus from Australia is a significant risk if backdoors are mandated. This would also force entrepreneurs wishing to start businesses in IT to weigh up their options and potentially move to a country where the right to run strong encryption is still legal, such as the US where encryption is protected under the First Amendment. Providing customers strong protection for their communications is a major

---

[9] http://fortune.com/2018/01/10/goldman-sachs-bitcoin-currency/
[10] https://www.engadget.com/2017/12/08/australian-securities-exchange-blockchain-march-2018/
[11] http://www.nasdaq.com/article/7-most-interesting-uses-of-blockchain-cm875394
[12] http://www.digitalistmag.com/digital-economy/2017/12/19/using-blockchain-for-media-rights-management-ad-revenues-05644369
[13] https://www.mivote.org.au/what_is
[14] https://voteflux.org/
[15] https://www.afp.gov.au/what-we-do/crime-types/fraud/identity-crime
[16] https://arstechnica.com/tech-policy/2015/06/software-companies-are-leaving-the-uk-because-of-governments-surveillance-plans/

selling point and providing end to end encryption could be the difference between a start-up enterprise succeeding or failing.

The development of blockchain technology has the promise of changing the way the world does business, built on unbreakable encryption. The potential for innovation in this space is huge. If the government mandates rules around encryption, Australia runs the risk of becoming a financial backwater as developers will be forced to work elsewhere and businesses may have to forego opportunities presented to them using these new tools. An unfortunate policy decision by the Australian Tax Office regarding the GST implications of cryptocurrency transactions saw some Australian businesses immediately relocate to other countries[17]. Similar consequences should be expected in the information security industries, if the government goes down the path of weakening or attempting to backdoor encryption technologies, products, or protocols.

Australian leadership in the information age

Australian legislators have already made countless mistakes in attempting to regulate the Internet, continuously granting sweeping new powers to LEAs against the advice of Internet technology experts and civil society organisations. Australian legislators need to make a policy choice regarding whether they wish to pursue cyber-war or cyber-peace. Building offensive hacking teams inside the Australian Signals Directorate, deploying the Australian Secret Intelligence Service against the East Timor government for the commercial benefit of Australian gas corporations[18] etc. are examples of Australia throwing away any moral authority this nation could have to lead peaceful and secure Internet policy development in our region.

Australians, like millions of people all around the world, are turning to encryption as the last defence they have for their human right to privacy given the wholesale abandonment of privacy rights by western intelligence agencies, as revealed by Edward Snowden.

Pirate Party Australia encourages the committee to use this inquiry to recommend a change in the way Internet policy is legislated in Australia. Instead of challenges face by LEAs being used as an opportunity to grant them even greater powers, new approaches to Internet policy development should first be found by legislators to rebuild the trust citizens are losing in their governments.

[17] http://www.zdnet.com/article/australias-coinjar-moves-hq-to-uk-for-progressive-bitcoin-scene/
[18] https://www.theguardian.com/world/2013/dec/03/timor-leste-spy-witness-held-lawyers-office-raided-asio