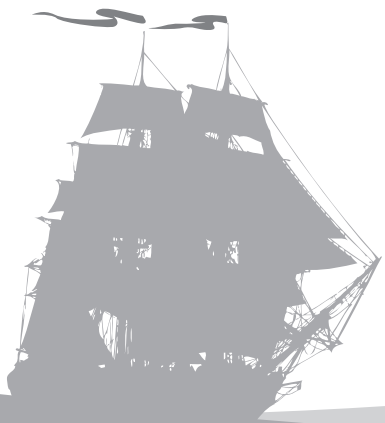
pirateparty australia

Submission to the Parliamentary Joint Committee on Intelligence and Security Inquiry into potential reforms of National Security Legislation

Simon Frew (simon.frew@pirateparty.org.au)
Benjamin McGinnes (ben@adversary.org)

August 2012



Contents

Introduction

We would like to take this opportunity to thank the PJCIS for the opportunity to make a submission to the National Security Inquiry. Since the beginning of the War on Terror, there have been almost yearly expansions of the powers of Australia's security services. This is the first real opportunity the public have been given to respond to the consistent erosion of our civil liberties. We hope that the members of the Committee will take into account the widespread opposition to the expansion of surveillance and reject the proposals that threaten the civil liberties and privacy of all Australians.

Of particular concern is the short time frame that the public has been given to respond to the inquiry. Whilst an extension was made after the outcry with the August 6 deadline, there still has not been sufficient time to deal adequately with such a complex, lengthy and important issue. Much of what is proposed has not been adequately explained or justified, which has added to the difficulty in formulating a comprehensive response to what are already very complex issues.

Due to the broad nature of the review, areas not listed in our submission are either directly addressing the committee or those on which we have no firm opinion and can offer no advice.

Where terms and acronyms have not been explained in this document, the glossary used in the discussion paper has been used. All headings in the table of contents, citation numbers and URLs function as links.

2) The inquiry should consider the effectiveness and implications of the proposals to ensure law enforcement, intelligence and security agencies can meet:

a) The challenges of new and emerging technologies upon agencies' capabilities

Central to the justification for the sweeping new powers being advanced by the Security Services is that they need to adapt to the changing telecommunications landscape to keep pace with criminals. While there is some need to modernise surveillance powers, many of the proposals assault basic freedoms currently enjoyed by Australians and go far beyond any measure of equivalency with powers previously exercised by the state.

Interception powers need to remain carefully balanced with the right to privacy for Australian citizens. Changes to the *Telecommunications (Interception and Access) Act 1979* (TIA Act) need to be made with this in mind. Laws mandating targeted interceptions based on strict warrant conditions and proper judicial oversight should be made to address any decline in the ability of security services to investigate crime.

Pirate Party Australia believes that only crimes of a serious nature, with a minimum gaol time of 7 years would justify the use of surveillance technologies as stipulated in the TIA Act. Reducing the severity of crimes for which surveillance can be deployed

will lead to greater surveillance of society at large and will impact upon civil liberties in Australia (see below).

b) The requirements of a modern intelligence and security agency legislative framework, and to enhance cooperation between agencies

There is some need for security agencies to be able to co-operate more effectively. Espionage, terrorism, people smuggling, etc. all have transnational elements that require cooperation by foreign intelligence services (e.g. ASIS) and locally based intelligence services (e.g. ASIO). There is also need for co-operation in Australia between different intelligence services.

Where this gives us rise for concern is the possibility that enhanced co-operation could be used for "power shopping" i.e. working with the agency with the lowest thresholds of accountability to avoid proper scrutiny.

There is also concern that enhancing co-operation while reducing the number of agencies able to carry out surveillance is just an exercise in obfuscation, generally increasing the amount of surveillance carried out, albeit by fewer agencies. If this is the case, it must be resisted by the Committee.

c) The need for enhancements to the security of the telecommunications sector.

This is an important proposal. While there is no such thing as a completely secure system, the telecommunications sector must do what they can to minimise the risks to their systems and their private customer data. Specific proposals shall be addressed below.

3) The Committee should have regard to whether the proposed responses:

a) contain appropriate safeguards for protecting the human rights and privacy of individuals and are proportionate to any threat to national security and the security of the Australian private sector

The backdrop for the sweeping new powers proposed is a consistently falling rate of crime across the community. According to the Australian Institute of Criminology report, *Australian Crime: Facts and Figures 2011*[1], the rate of crime is on the decline. Most notably, there has been a massive drop in all forms of property crime with a halving of both motor vehicle theft and break and enters since a peak around the turn of the millennium. All categories with the exception of kidnapping have also seen declines

[1] Australian Institute of Criminology, *Australian crime: Facts & figures (2011)*, http://www.aic.gov.au/documents/0/B/6/%7B0B619F44-B18B-47B4-9B59-F87BA643CBAA%7Dfacts11.pdf.

over the last few years, albeit not to the same degree as property crime. In any case, current policing powers are working effectively and we see absolutely no justification for granting Security agencies any new powers beyond their current capabilities.

The right to privacy is a civil right, defined as such in the International Covenant on Civil and Political Rights[2], entered into force in Australia on November 13th, 1980. It specifically mentions arbitrary interference with privacy in Article 17 of the Covenant. The proposals to widen the scope of crimes that surveillance can be deployed to investigate and data retention are a direct assault on this right. They make suspects of us all, destroying once and for all the concept of being innocent until proven guilty by placing everybody under surveillance, regardless of suspicion or need. It is an arbitrary (rather than discriminating) violation of privacy and contrary to the Covenant.

The discussion paper alludes to society having a lower expectation of privacy than it has in the past and uses this claim to blunt the arguments of privacy advocates. This comes from the information people share about themselves on social media (Facebook, Twitter, etc). We should not conflate choosing to share with giving up the right to privacy; they are not the same thing. A survey of Facebook users[3] shows that only 36% of the content posted on Facebook is considered public by the posters. What people share with friends online is not public information, it may be more information than they shared with their friends in the past, but there was no ability to share your photos, your thoughts or your interests except through face to face contact or by physical mail. What has not changed is the desire for everyone to retain control over their personal information. Consequently the assumption that a lower perceived expectation of privacy stemming from current social media usage is falsely equated with an argument for a reduced right to privacy.

People under constant surveillance stop behaving like free people; to the detriment of society. Data retention plans similar to the proposed regime in the terms of reference have been enacted in Europe under the Budapest Convention on Cybercrime[4] to widespread opposition, with legislation being rejected by Sweden and overturned in Germany, Romania and the Czech Republic as unconstitutional. In the German case the Judges determined that blanket surveillance could ”cause a diffusely threatening feeling of being under observation that can diminish an unprejudiced perception of one’s basic rights in many areas,” as stated by the President of the Court, Hans-Jürgen Papier. They considered that ”such retention represents an especially grave intrusion” into citizens’ privacy[5].

The German data retention regime, while it was implemented, had a negative impact upon people accessing online resources due to privacy concerns. Research institute Forsa found that one in two Germans would refrain from seeking help from professionals such as marriage and drug abuse counsellors and psychotherapists by telephone, mobile phone or email because of privacy concerns. One in thirteen people had already refrained from using telecommunications at least once due to data retention, which put

[2] *International Covenant on Civil and Political Rights*, http://www2.ohchr.org/english/law/ccpr.htm.

[3] Attorney-General’s Department, *Telecommunications (Interception and Access) Act 1979 - Annual Report for the year ending 30 June 2011*, http://www.ag.gov.au/Publications/Pages/Telecommunications(InterceptionandAccess)Act1979AnnualReportfortheyearendingJune2011.aspx.

[4] *Convention on Cybercrime*, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[5] EDRI, *German Federal Constitutional Court Rejects Data Retention Law*, Mar. 10, 2010, http://www.edri.org/edrigram/number8.5/german-decision-data-retention-unconstitutional.

the number at an estimated 6.5 million people[6]. The negative impact on the health and wellbeing of citizens caused by the lack of privacy should be reason alone to reject the data retention proposal.

The fear of what you look up and view in your own home, who you communicate with and what you say becoming publicly available is well founded. The collection of private data creates targets for those wishing to exploit the data for nefarious means.

Recently, more than one major Australian Telco has breached the privacy expectations of their customers. Telstra sent customers web browsing histories to a Canadian company against its own Terms of Service[7]. The company has since stopped the practice amid outrage, apologising for it and promising to do better[8]. AAPT had 40 gigabytes of customer information stolen recently in protest of this very proposal[9]. In the UK employees of T-Mobile sold the personal data of seventeen million customers[10].

The danger of private information being stored by ISPs becoming public is real. Similarly, there is also a significant danger with any data being stored by Australia's security services. The case of Canadian spy Jeffrey Paul Delisle selling classified Australian information to Russia[11] shows just how vulnerable such private information is. The ease with which foreign powers could turn Australian citizens into informants through blackmail by having access to their most personal records is of great concern. The safest thing to do to protect Australians from privacy breaches, which in turn protects our national security, is by not capturing and storing the data at all.

Another disturbing proposal in the terms of reference is the creation of a prison penalty for "failure to assist in the decryption of communications" which is a direct assault of a person's right to remain silent when being questioned or placing a person at risk of criminal charges for failing to perform a task that is beyond their control (see below for details).

b) Apply reasonable obligations upon the telecommunications industry whilst at the same time minimising cost and impact on business operations in the telecommunications sector and the potential for follow on effects to consumers, the economy and international competition

Mandatory data retention would place significant costs on ISPs, social media platforms and websites operating in Australia. The sheer size of the data set that would need to be retained by companies operating in the digital environment is staggering. In the

[6] forsa, *Meinungen der Bundesburger zur Vorratsdatenspeicherung [Opinions of citizens on data retention]*, June 2, 2008, http://www.webcitation.org/5sLeT8Goj.

[7] Ben Grubb, *Telstra accused of Next G web 'stalking'*, July 5, 2012, http://www.smh.com.au/technology/technology-news/telstra-accused-of-next-g-web-stalking-20120705-21ivs.html.

[8] Ben Grubb, *'Customer privacy is not negotiable': Telstra boss admits leaking customer data*, July 6, 2012, http://www.smh.com.au/technology/technology-news/customer-privacy-is-not-negotiable-telstra-boss-admits-leaking-customer-data-20120706-21lzo.html.

[9] Joel Falconer, *Anonymous hacks Australian ISP AAPT to demonstrate data retention problems*, http://thenextweb.com/au/2012/07/26/anonymous-hacks-australian-isp-aapt-to-demonstrate-data-retention-problems/.

[10] Barry Collins, *T-Mobile admits selling customers' mobile records*, Nov. 17, 2009, http://www.pcpro.co.uk/news/353377/t-mobile-admits-selling-customers-mobile-records.

[11] Philip Dorling, *Foreign spy 'stole' Australian secrets*, July 25, 2012, http://www.theage.com.au/opinion/political-news/foreign-spy-stole-australian-secrets-20120724-22nl6.html.

Quarter to June 2011 it was estimated Australians downloaded 274,202 Terabytes (TB), or in analogue terms, 167.5 million libraries of 10,000 books each[12]. The amount of data is massive, growing rapidly and it will have a further expansion once the National Broadband Network is deployed. Whilst not all of the data will need to be stored, the amount of data that will need to be sifted through and stored is enormous.

The costs resulting from the warehouses of servers required to store the data would place a significant burden on affected companies and consequently their consumers. There is a real risk that such an onerous provision could prohibit any new businesses from entering the market due to the high costs associated with meeting the data retention requirements.

c) Will address law enforcement reduction of capabilities from new technologies and business environment, which has a flow-on effect to security agencies.

The biggest issue facing surveillance powers of Australia's security agencies is the diversification of communications platforms and subsequent difficulties intercepting the communications.

With proper judicial oversight, serious crimes (those attracting a minimum sentence of 7 years or more) can be investigated through telecommunications intercepts. Where capabilities exist, such as ISPs, targeted data of suspects should be permitted to be stored and accessed by Australia's security services and law enforcement.

Attempting to access private communications of people that take place on social networks and similar platforms poses many issues which need to be carefully weighed before any legislation demanding access to data can be advanced.

- The right to privacy for other individuals needs to be protected from abuse by investigating officers. Blanket access for fishing expeditions can cause many innocent people to have their privacy invaded.
- Whether Australia has any jurisdictional ability to access the information.
- The ability of the site operator to comply with requests. Many bulletin boards, blogs, etc. are run by amateur operators who do not have the resources or quite possibly the technical understanding to grant access to the private data of members.

The National Security Legislation, the subject of the inquiry, has three different elements and Objectives. They relate to:

• Modernising lawful access to communications and associated communications data

This is discussed throughout the submission. We agree with this objective only as far as it remains in line with current checks and balances. Any attempt to widen the basis of data access must be rejected.

[12] Australian Communications and Media Authority, *Chapter 1 - The Australian communicationsand media market*, 2011, http://www.acma.gov.au/webwr/_assets/main/lib410148/chapter%201_the_aus_communications_and_media_market.pdf.

• Mitigating the risks posed to Australia's communications networks by certain foreign technology and service suppliers

Communications networks are key targets for attackers as they are a central point at which data from government, private businesses and civilians can be easily intercepted in transit and transmitted to an overseas location for further analysis. Such systematic collection of data may allow foreign attackers to glean information on individuals which in turn can be used to harass or blackmail them, and can lead to more serious consequences such as the leaking of trade secrets and confidential government data which could threaten Australian industries and national security.

The communications ecosystem is a patchwork of multiple hardware suppliers, software solutions and both in-house and outsourced engineering and construction expertise. We currently possess neither the product design nor manufacturing expertise to create such solutions from scratch locally so C/CSPs and ISPs in Australia utilise technology and services supplied externally from companies in Asia, Europe and the USA[13].

Currently, most C/CSPs and ISPs source technology and service solutions, trusting that the vendor will act in good faith and deliver a virgin product. With the construction of the National Broadband Network, vendors with malicious intentions have a prime opportunity to target the entirety of Australian telecommunications networks by supplying equipment containing illegal interception capabilities.

Several of the largest communications solutions vendors supply equipment to countries with oppressive government regimes, with the capabilities to track civilians' activities on the internet, intercept and inspect data in transit[14] and censor ideologically unsuitable content. For example, Cisco Systems, an American networking equipment specialist supplies core routing equipment to the government of the People's Republic of China for use in their 'Golden Shield' project[15] to enforce censorship and track members of religious movements for the express purpose of persecuting them.

It would be naïve to assume that suppliers based in countries with which Australia has an alliance, or is politically neutral to, would be averse to modifying equipment for the purpose of intercepting Australian communications. Just as it is feasible for such capabilities to be added at the request of the customer, it is equally feasible for the same capability to be added covertly at the request of a foreign power, especially when some vendors (e.g. Huawei) have ties to military forces[16]. It is based upon such reasoning that the Attorney General's Department has already banned Huawei from supplying core components for the construction of the National Broadband Network, citing national security fears on advice from ASIO[17].

[13] Renai LeMay, *Govt bans Huawei from NBN tenders*, Mar. 24, 2012, http://delimiter.com.au/2012/03/24/govt-bans-huawei-from-nbn-tenders/.

[14] C. Sharp F. Baker B. Foster, *Cisco Achitecture for Lawful Intercept in IP Networks*, 2004, https://www.ietf.org/rfc/rfc3924.txt.

[15] Asher Moses, *Fighting China's Golden Shield: Cisco sued over jailing and torture dissidents*, Aug. 16, 2011, http://www.smh.com.au/technology/technology-news/fighting-chinas-golden-shield-cisco-sued-over-jailing-and-torture-of--dissidents-20110816-1ivkv.html.

[16] Peter Hartcher, *Why ASIO won't get online with Huawei*, Apr. 10, 2012, http://www.smh.com.au/opinion/politics/why-asio-wont-get-online-with-huawei-20120409-1wl2y.html.

[17] Renai LeMay, *Govt bans Huawei from NBN tenders*, Mar. 24, 2012, http://delimiter.com.au/2012/03/24/govt-bans-huawei-from-nbn-tenders/.

Vendors have an existing track record of such nefarious behaviour. For example, RuggedCom, a Canadian supplier of industrial automation controls which are widely used internationally to monitor and control critical utilities, such as power grids, pipelines and substations, military installations and traffic control systems was discovered to have implemented a back door in their operating system[18]. This back door was easily exploitable and hard coded into every system produced. This was not discovered initially as the devices were never audited comprehensively and the company did not disclose this information to their clients. In a similar case, Linksys, the consumer arm of Cisco Systems which manufactures networking equipment which ISPs supply to civilians for home use, configured a setting by default which allowed them to modify and upgrade the device's functionality at their will, and to track the Internet usage of users. This constitutes a serious invasion of privacy and such a feature could be manipulated by a foreign supplier or state-sponsored attacker to survey the activities of Australian citizens and small businesses[19].

Steps can be taken to minimise the risks to Australia's communications networks:

- Where possible, select locally developed and manufactured solutions over those supplied by foreign companies.
- Where possible, limit construction and engineering tenders to Australian firms.
- Employ Australian labour rather than outsourcing work to companies with offshore employees.
- Require all data pertaining to communications networks, and all data stored as part of the functioning of communications networks to remain in Australia (that is, in Australian data centres and not overseas, where it may be subject to the laws of another jurisdiction or tampered with).
- Mandate security screening of all personnel with high level access to communications networks.
- Enforce physical access controls to critical infrastructure.
- Create a comprehensive framework to guide C/CSPs and ISPs in regular audits of communications networks, documentation of any modifications and the reporting of suspected breaches to relevant government authorities.

Australian universities and industry train many competent electrical, telecommunications and software engineers who have the skills to assess hardware and software solutions sourced from foreign suppliers for security risks or back doors introduced by the suppliers for malicious purposes.

Vendors should be required to provide the underlying source code of any product, full technical specifications, engineering data, schematics and diagnostic information to the government. This can then be used by Australian citizens with appropriate security clearances to audit the supplied solution for any security flaws and verify there has been no attempt to interfere with the products advertised function by foreign powers. If possible, vendors should also be required to build in a failsafe system that allows rapid verification of the solutions integrity, such that the government, C/CSPs and ISP are

[18] Dan Goodwin, *Backdoor in mission-critical hardware threatens power, traffic-control systems*, Apr. 25, 2012, http://arstechnica.com/business/2012/04/backdoor-in-mission-critical-hardware-threatens-power-traffic-control-systems/.

[19] Joel Hruska, *Cisco's cloud vision: Mandatory, monetized and killed at their discretion*, July 2, 2012, http://www.extremetech.com/computing/132142-ciscos-cloud-vision-man.

not burdened with the lengthy and expensive process of verifying each individual unit delivered.

Such a rigorous inspection process is the only method to minimise the risk posed to communications networks. As a side benefit, any product flaws that the vendor has not discovered can be reported so they may be rectified immediately.

Some vendors, such as Huawei have offered the source code upon request to governments for inspection to alleviate security fears, as well as access to independent third parties for auditing[20]. Certification and security clearance of Huawei staff is also offered as an option. Governments from countries such as the United Kingdom, New Zealand and India have taken advantage of such programs in the certification of Huawei hardware for installation in their communications networks.

Pirate Party Australia believes risks to Australia's communications networks can be minimised with the allocation of resources such that all technology and services supplied by foreign suppliers to C/CSPs, ISPs and industry can be effectively screened before deployment and regularly reassessed.

• Enhancing the operational capacity of Australian intelligence community agencies.

This should only be done in relation to modernising communication interception legislation in line with current powers. Due to falling crime rates and a claimed four terrorist attacks prevented[21] under the current system, we see absolutely no justification whatsoever in reducing freedoms and civil liberties of Australians in order to enhance the operational capacity of any intelligence organisation.

A) Government wishes to progress the following proposals:

Telecommunications (Interception and Access) Act 1979

1. Strengthening the safeguards and privacy protections under the lawful access to communications regime in the Telecommunications (Interception and Access) Act 1979 (the TIA Act). This would include the examination of:

a. The legislation's privacy protection objective

The TIA Act protects the privacy of people not suspected of a serious crime. A specific provision guaranteeing the preservation of privacy of individuals not suspected of any serious crime would be warmly applauded. The right to privacy is a civil right, defined as such in the International Covenant on Civil and Political Rights[22], entered into force

[20] Kathrin Hille, *Huawei seeks to overturn Australian ban*, Mar. 26, 2012, http://www.ft.com/cms/s/0/bd360448-7733-11e1-baf3-00144feab49a.html.

[21] Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats Discussion Paper*, 2012, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/additional/discussion%20paper.pdf.

[22] *International Covenant on Civil and Political Rights*, http://www2.ohchr.org/english/law/ccpr.htm.

in Australia on November 13th, 1980. It is fundamental to the continuance of a free and democratic society.

b. The proportionality tests for issuing of warrants

There must be no weakening of protections through widening the scope of interception activities through reducing the minimum gaol term provision below seven years or widening the list of crimes that surveillance can be deployed to investigate (see terms of reference A2b, B8a and C14a).

There is absolutely no justification of increased risk, nor crime wave to justify granting security agencies any powers beyond those they currently enjoy. If there were an increased risk it would still be not advisable to grant extra powers because every new power granted to security agencies weakens those few civil liberties enjoyed in this country. It reduces the very freedoms they are meant to protect.

c. Mandatory record-keeping standards

The proposals here for the most part are common-sense. However, there are practical issues with some of the telecommunication carriers and carriage service providers (C/CSPs) as defined in the discussion paper.

Virtual Private Networks (VPNs) are used by individuals who need to be sure of confidentiality and security. While record keeping would provide security agencies with records of communications, they weaken the effectiveness of these services, many of which guarantee privacy by not keeping records at all. Forcing these service providers to keep records will weaken their services and force people to use similar services based outside of Australia's jurisdiction or use other anonymising products, of which there are a plethora.

There are legitimate needs for privacy online, particularly with lawyers, journalists, medical professionals and businesses conducting commercial in-confidence negotiations or exchanges.

d. Oversight arrangements by the Commonwealth and State Ombudsmen

Whilst this is mentioned in the discussion paper, it is unclear what exactly is being proposed. It seems reasonable to keep the Commonwealth Ombudsman overseeing all Law Enforcement Agencies Australia wide, to ensure oversight within Federal limits, and retain State Ombudsmen to oversee State aspects of Law enforcement. Likewise the Inspector General of Intelligence and Security (IGIS) would continue to perform a similar role in regards to the intelligence services. We see no reason to adjust the current arrangement.

2. Reforming the lawful access to communications regime. This would include:

a. Reducing the number of agencies eligible to access communications information

Reducing the number of agencies and organisations with access to interception is good, but it raises a number of questions.

- Which groups will continue to have access to this power?
- Is this a bit of a shell game if ASIO will be granted an increased ability to cooperate with other

- organisations within the community (including businesses)?
- Will other changes to telecommunications interception (TI) warrants effectively grant greater power under the guise of reducing access to a small subset of agencies?

The terms of reference specifically refer to "reducing the number of agencies eligible to access communications information" and not to reducing the number of agencies eligible to intercept communications. This indicates that the agencies which will lose their authority over communications will only be those which currently do not have any interception powers at all.

This means that the 17 State and Commonwealth agencies[23] referred to on page 24 of the discussion paper will retain all the powers to be granted under these proposals, as will Royal Commissions.

Those organisations which currently have the power to request a stored communications warrant and from which this power will be removed will probably push for the return of those powers in the future, after the scope of such warrants has been significantly expanded.

This raises a number of issues:

- What safeguards can and will be put in place to prevent these expanded powers being granted to those
- organisations from which it was removed?
- There will be nothing to prevent future amendments to legislation granting to warrants for both interception and access to stored communications to those organisations.

If these expanded powers were to be granted to non-law enforcement or non-intelligence organisations at some stage in the future, it would place an unprecedented amount of power with bodies not designed to handle that power. These organisations would likely be lacking the systems and oversight necessary to ensure correct handling of the information which would be available from these powers.

Many of these organisations, like Centrelink, do not have the best track record for not abusing the powers and access to information that they already have[24]. Some organisations have had public confidence in them significantly eroded after privacy breaches occurred, compromising data they were entrusted with. The distrust is at a point where future moves to expand their powers – by "restoring" those powers removed from them under the proposed changes – would only further entrench this justified distrust of public institutions.

As a consequence, legislation is required to prevent agency scope creep. Removal of powers to access stored communications must be coupled with permanent safeguards against the granting of even greater powers in the future. Should the government fail in this task, then that failure will be indicative not of an attempt to streamline the surveillance powers of law enforcement and intelligence, but rather lay the foundations for the

[23], ASIO, the Australian Federal Police, State and Territory police forces, police integrity and anti-corruption organisations, the Australian Crime Commission and CrimTrac.

[24] Liam Tung, *Staff sacked after widespread privacy breaches at Centrelink*, Sept. 26, 2007, http://www.zdnet.com/staff-sacked-after-widespread-privacy-breaches-at-centrelink-1339282381/.

construction of a sweeping surveillance state which is prepared to pry into the lives of every single Australian.

Even with legislation designed to prevent agency scope creep there remains the possibility of these safeguards being removed by future legislative amendments. Any attempt to do so would be a clear indication of the same lack of commitment to streamlining surveillance powers and a broad policy of snooping on the populace.

b. The standardisation of warrant tests and thresholds

This proposal, in conjunction with the previous proposal to reduce the number of agencies with access to TI powers and warrants (A2a), feeds directly into enabling the proposal to create a single warrant with multiple interception powers (B8a).

The current threshold for obtaining a warrant to intercept real time communications is investigation of a serious crime with a penalty of 7 years in prison or greater while the threshold for obtaining a warrant to access stored communications is a crime with a penalty of 3 years in prison or greater.

The proposal recommends lowering the threshold, but does not explicitly state what they want the threshold to be lowered to. The implication of proposing a new warrant with multiple TI powers (B8a), merging the interception and access to stored communications, is that the minimum threshold would be for crimes with a penalty of 3 years in prison or greater.

This proposal cites an apparent disparity between the thresholds and certain types of crimes for which law enforcement would like to be able to obtain TI warrants. The specific example in the discussion paper being child exploitation offences.

The existence of such a disparity or the perceived existence of such a disparity does not ipso facto mean that the thresholds should be lowered to address this. There are alternative courses of action.

Should such a disparity, following a proper review, be determined to exist, the particular crimes not meeting the existing thresholds could be included by raising the penalties for those crimes (e.g. child exploitation offences) to a level where the crimes would meet the threshold. Alternatively, the disparity could be addressed by making the threshold a serious offence (punishable by 7 years or more) or a specific list of offences which do not meet that threshold, but which are still considered serious enough to justify an interception, such as child exploitation offences.

Such a list of offences for which an exception might be made would need to be limited and additions to such a list should require both judicial oversight and legislative amendment with a public inquiry. If law enforcement believe that the disparity is reflected by community values then that will be reflected by public submissions to those inquiries.

Pirate Party Australia does not believe that the thresholds for telecommunications interceptions should be lowered from serious crimes with a penalty of 7 years or greater in prison. Furthermore, the changing nature of what constitutes stored communications and the potential sensitivity of those communications should also be subject to the threshold for serious crimes. The reason being that stored communications are often just as sensitive as real time communications, if not more so.

3. Streamlining and reducing complexity in the lawful access to communications regime. This would include:

a. Simplifying the information sharing provisions that allow agencies to cooperate

This proposal reduces administrative paperwork, favouring record keeping for 'recording the information needed to ensure that a particular agency's use of intrusive powers is proportional to the outcomes sought.'[25] Part of the justification for this change is "... many of the requirements reflect historical concerns about corruption and the misuse of covert powers and do not reflect the current governance and accountability frameworks within which agencies operate."

While better information about the proportionality of the use of an agency's intrusive powers is important and necessary, there is no diminished concern in the community regarding corruption in Australia's political institutions and law enforcement agencies. Notably, in 2008, both Wollongong City Council[26] and Shellharbour Council[27] were sacked by the NSW State Government for systemic corruption.

We support security agencies providing more relevant information about the proportionality of any use if their invasive powers, while opposing any streamlining that reduces the ability of investigative bodies to uncover corruption or abuse of power.

b. Removing legislative duplication

Pirate Party Australia supports this proposal, so long as each consolidation retains the standards in both sets of the consolidated version of the law.

4. Modernising the TIA Act's cost sharing framework to:

a. Align industry interception assistance with industry regulatory policy

Pirate Party Australia has no position on this item.

b. Clarify ACMA's regulatory and enforcement role

The current powers accorded to ACMA are adequate to enforce TIA powers upon telecommunications providers. Contrary to the implication of the proposal, we see no reason for such provisions to be exercised publicly in a court of law. The only reason we believe this proposal is being put forward is a cultural opposition to any form of transparency or oversight within Australia's Intelligence Agencies.

[25] Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats Discussion Paper*, 2012, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/additional/discussion%20paper.pdf.

[26] ABC News, *Sack Wollongong Council: ICAC Commissioner*, Mar. 3, 2008, http://www.abc.net.au/news/2008-03-03/sack-wollongong-council-icac-commissioner/1060724.

[27] Sarah Allely, *Shellharbour Council sacked*, July 9, 2008, http://www.illawarramercury.com.au/news/local/news/general/shellharbour-council-sacked/807820.aspx.

Australian Security Intelligence Organisation Act 1979

5. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions

a. To update the definition of 'computer' in section 25A Pirate Party Australia supports consistency of definitions and accurate definitions across Australian legislation (see also B11b).

b. Enabling warrants to be varied by the AG, simplifying the renewal of the warrants process and extending duration of search warrants from 90 days to 6 months.

All warrant powers must be overseen by a competent judicial officer, not a minister. Separation between the government and judiciary must be maintained. We believe judicial oversight should be mandatory for any variation or extension of a warrant to ensure the powers of the security agencies are not abused.

While the Committee members may be comfortable granting the current Attorney-General such powers, they remain for every future politician. Similar powers have been used by authoritarian regimes to persecute members of the opposition (a recent example of such abuse of power can be seen with the Chavez regime in Venezuela[28]) and the risk of this happening in Australia must be avoided.

6. Modernising ASIO Act employment provisions

This section is reasonable and we see no reason to object to any provisions.

Intelligence Services Act 2001

7. Amending the Intelligence Services Act 2001 to clarify the Defence Imagery and Geospatial Organisation's authority to provide assistance to approved bodies.

We support the Defence Imagery and Geospatial Organisation having the authority to provide assistance to approved bodies. We believe that some unclassified information should be released to the general public in part to build confidence with the Australian Intelligence Community (AIC), and in part to satisfy public interest in such research.

[28] Human Rights Watch, *Venezuela: Concentration and Abuse of Power Under Chavez*, July 17, 2012, http://www.hrw.org/news/2012/07/17/venezuela-concentration-and-abuse-power-under-ch-vez.

B) Government is considering the following proposals:

Telecommunications (Interception and Access) Act 1979

8. Streamlining and reducing complexity in the lawful access to communications regime – this would include:

a. Creating a single warrant with multiple TI powers

On the face of it this proposal appears to be geared towards streamlining a convoluted warrant process. It does, however, provide the possibility of enabling a greater level of surveillance than currently employed.

This proposal is clearly linked to the previous proposal to reduce the number of agencies with access to TI powers (A2a). The agency reduction may have even been proposed in order to facilitate the possibility of this proposal being adopted.

This proposal is also linked to the previous proposal to standardise the warrant tests and thresholds (A2b). Such standardisation would make it possible to grant all the interception powers enabled by a single warrant with TI powers.

The current regime splits powers in a manner which sees some suspects under investigation able to have a part of their communications intercepted without enabling a massive level of invasion which could easily affect those around them, such as friends and family with no connection to the matter for which the suspect is being investigated. By creating a single warrant with multiple powers, anyone suspected of anything for which a TI warrant is granted will have the full range of TI powers automatically approved for use against them, regardless of whether they meet the thresholds that would have previously been applied for that degree of invasive interception.

If this single warrant retains a threshold test for serious crimes (with a penalty of 7 years or greater imprisonment) then there should be no obstacle in implementing it. If, however, the threshold is lower than that then there would be grave concerns in allowing it.

9. Modernising the Industry assistance framework –

a. Implement detailed requirements for industry interception obligations

In the terms of reference C16A, the costs of securing a network are expected to be borne by the telecommunications industry. This is reasonable because it is in the best interest of both the company and their customers to have a secure system. However, interception activities have no flow through benefit for customers or the company (see the section of civil liberties above Committee Responsibilities 3A and the mandatory retention section C15C below for the dangers of these proposals). Pushing the cost of data retention onto the subscribers of a service makes them pay more for a lesser service. This will rightly cause the resentment of Australia's Internet users.

The government should bear the costs of any data retention ordered in the investigation of a crime. It is not the duty of companies to fund the works of Australia's intelligence services except, like everyone else, through the payment of taxes.

Mandatory data retention as proposed in C15C will be a massive undertaking, costing billions of dollars in server upgrades, backups and extra security (not counting all the lawsuits when security is breached and millions of customers' data exposed). With over one million terabytes of data and rising being downloaded by Australians every year (see Committee Responsibilities 3B for details), the cost of storing the data would be a significant imposition upon the service providers and subsequently their customers. To paraphrase Tony Abbott; this is a great big new tax on all Internet users.

Targeted data retention of suspects' information under a strict warrant regime would be a much more cost effective measure, without the serious implications for civil liberties of the blanket data retention proposal. Such a system would be significantly more cost effective than retaining all Internet user data, and while we believe all costs of law enforcement should be borne by the state, such a regime would not unduly burden ISPs and other stakeholders in the telecommunications sector.

b. Extend the regulatory regime to ancillary service providers not currently covered by the legislation

This proposal is particularly problematic due to the global and distributed nature of the Internet. Most obviously are questions of jurisdiction. Millions of Australians access sites based in other countries every day. They are not necessarily subject to Australian law and therefore no law requiring Australian customer data be kept could be enforced. Sites in Australia too have millions of users based in other countries. Expecting these companies to comply with data retention directives could force them offshore, or alternatively force them to store millions of data sets of no interest to the AIC or law enforcement. This could seriously harm the international competitiveness of Australian web services.

Many Australian Internet services, including some ISPs (e.g. APANA member nodes), operate on a not-for-profit basis. Imposing data retention costs on these organisations, which can have hundreds of thousands of users, is overly burdensome and limits their effectiveness for very little security benefit. This would impose both a technical and economic cost on anyone wishing to run their own Internet services (e.g. shell/terminal access for developers around the world, free email services, etc). Many popular sites are run by their creators who just use templates to set things up. These people don't have the money, the technical knowledge or time to deal with requests for customer data from security services. As a consequence these law abiding people may choose to either cease operating their sites or engage the services of an offshore provider which does not need to concern itself with Australian law.

More important than the cost and technical issues, the civil liberty issues of such a regime are dangerous to the liberties currently enjoyed by the Australian population. Whilst some content posted on social media may be considered for public consumption, the majority of the material is considered privately shared amongst friends (See our response to Committee Responsibilities 3A for details). A real world equivalent would be a Friday night at the local pub. It is not possible for security services to record the conversations out on a Friday night, regardless of what is being discussed. This same kind of privacy should be expected in social media forums online.

c. Implement a three-tiered industry participation model

A tiered model specifically for telecommunications providers, based upon the size and structure of the businesses, is useful for helping security services ensure Australia's information networks are secure.

Australian Security Intelligence Organisation Act 1979

10. Amending the ASIO Act to create an authorised intelligence operations scheme. This will provide ASIO officers and human sources with protection from criminal and civil liability for certain conduct in the course of authorised intelligence operations.

This is a reasonable proposal as explained in the discussion paper so long as strict safeguards are in place. The controlled operations scheme as outlined in the Crimes Act 1914[29], along with the additional safeguards listed in the discussion paper should represent a template for any such powers being granted to ASIO. Any powers beyond what is explicitly spelled out in the Crimes Act could give rise to serious abuse and therefore should be avoided.

It is essential to guarantee that ASIO will not be permitted powers which would place them effectively above or beyond the law.

11. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions to:

a. Establish a named person warrant enabling ASIO to request a single warrant specifying multiple (existing) powers against a single target instead of requesting multiple warrants against a single target.

This proposal may be of some benefit with greater detail. If the concerns Pirate Party Australia has expressed over other provisions are addressed, particularly with regards to the thresholds and the powers granted by a warrant, then warrants targeting individual suspects may be of benefit to both ASIO or law enforcement and the community.

Safeguards must be in place to ensure that suspects are not subjected to undue harassment by being repeatedly subjected to searches of their home or person. Such abuse, which could be extended if used in combination with other proposals in the Inquiry paper (e.g. A5b granting Attorney-General discretionary powers over warrants) would result in a serious injustice.

b. Align surveillance device provisions with the Surveillance Devices Act 2007

Pirate Party Australia supports consistency of definitions and accurate definitions across Australian legislation (see also A5a).

c. Enable the disruption of a target computer for the purposes of a computer access warrant

This proposal enables ASIO or law enforcement to add, delete or modify any software or data on a computer system in order to execute a computer access warrant.

The language used is not specific to any particular purpose beyond accessing the targeted computer system, these provisions could be used to do anything to a targeted computer system in the course of gaining or retaining access to it. This could include anything imaginable and could be abused to a gross extent. This includes, but may not be limited to, any of or a combination of the following:

[29] *Crimes Act 1914 - Section 15GD*, http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/s15gd.html.

- Planting Trojan horse software[30], keystroke loggers[31], other malware[32] or other privacy-invasive software[33] on a targeted computer system.
- Removing any digital evidence of the planting of any kind of software or data on a targeted computer system.
- Planting incriminating information on a targeted computer system or device.
- Planting an encrypted file on the targeted computer system or device and then prosecuting the owner for being unable to decrypt that data following an order to do so under the decryption on demand legislation (C15a).
- Destroying data on a targeted computer system or device which a person might use to defend themselves during any prosecution.
- Accessing incriminating sites or services online from the targeted system to plant a false evidentiary trail in ISPs data retention records (C15c).
- Possibly extending these powers to third party computer systems or devices accessed to reach a targeted system in accordance with C17a.
- The computer system could be used as a bugging device by using built-in or connected cameras and microphones.
- If the computer system is used by people not targeted in the warrant this could result in collateral damage to their privacy and information.

If this power is aimed at a very particular task (e.g. planting Trojan horse software or a keystroke logger on a suspect's system which cannot be physically accessed or seized) and the Attorney-General's Department, ASIO or law enforcement wish to request it again, then that task must be explicitly specified in a future request and public inquiry. Such a power must be tailored in a manner which is restricted solely to that purpose with judicial oversight and controls on its use.

As it stands, Pirate Party Australia does not support this proposal. It would clearly grant vast power to ASIO and law enforcement to a degree that they have never before possessed. The potential for abuse of such power is phenomenal and must be avoided at all costs.

d. Enable person searches to be undertaken independently of a premises search

While there may be a legitimate need for this type of power, we need to be assured that it will not be open to abuse by enabling searches of anyone who is merely in the vicinity of a location specified in a warrant. Searches of people who are not under arrest (and may not be subject to arrest) are by their very nature invasive.

This power, if granted, must be restricted in order to prevent innocent members of the public becoming at risk of unnecessary stops and searches as a result of where they may be travelling. The power would need to be targeted through either a warrant to search that person, or possibly direct observation of that person exiting the location of a targeted premises immediately prior to the execution of a search warrant, or direct observation of that person exiting the location of a targeted premises during the execution of a search warrant.

[30] Wikipedia, *Trojan horse (computing)*, https://en.wikipedia.org/wiki/Trojan_horse_(computing).
[31] Wikipedia, *Keystroke logging*, https://en.wikipedia.org/wiki/Keystroke_logging.
[32] Wikipedia, *Malware*, https://en.wikipedia.org/wiki/Malware.
[33] Wikipedia, *Privacy invasive software*, https://en.wikipedia.org/wiki/Privacy-invasive_software.

There should be legislative safeguards for any other member of the public not covered by the above to be able to refuse such a search and to seek redress against ASIO or other law enforcement body involved in such a search should one occur unlawfully.

e. Establish classes of persons able to execute warrants

If the proposal is specifically restricted to the explanation in the discussion paper, i.e. to be able to stipulate classes of ASIO agents to execute a warrant, this is a reasonable adjustment to the ASIO Act.

12. Clarifying ASIO's ability to cooperate with the private sector.

While there can be arguments in favour of ASIO being able to cooperate with the business sector in order to satisfy its duties to protect Australian interests, including assisting Australian businesses which may be the target of foreign interference (numerous foreign powers utilise their intelligence services for economic gain), there is potential for such cooperation to be to the detriment of Australian society as a whole. Safeguards would need to be instituted to prevent Australian businesses from simply becoming an extension of the Australian Intelligence Community.

13. Amending the ASIO Act to enable ASIO to refer breaches of section 92 of the ASIO Act (publishing the identity of an ASIO officer) to authorities for investigation.

Pirate Party Australia has no problem with this specific amendment as long as it relates specifically to section 92 of the ASIO Act and not to any crime with a penalty of 12 months in prison or less.

C) Government is expressly seeking the views of the Committee on the following matters:

Telecommunications (Interception and Access) Act 1979

14. Reforming the Lawful Access Regime

a. expanding the basis of interception activities

There is no specific section in the discussion paper spelling out what is being proposed. There are provisions listed in other sections that fit in this heading so they will be addressed here.

The proposal to reduce minimum sentence time below the current threshold of seven years to encompass crimes for which the public expects surveillance to be deployed (the discussion paper cites child exploitation offences) will result in much more widespread use of surveillance.

Any surveillance of social media sites must be carried out with the most serious restrictions because any information linked to the social media account is also a part of every account holder they have connected with. An investigation of one account

exposes information that may not be public for every other account connected to the suspect.

Pirate Party Australia does not support providing carte blanche to law enforcement to expand the basis and reasons for conducting interception activities.

15. Modernising the Industry assistance framework

Establish an offence for failure to assist in the decryption of communications

There is very little information in the discussion paper on this proposal, only the inclusion of the idea in the terms of reference.

It is unclear what type or types of encrypted data the proposed legislation is directed at. It could be either or both of the following:

- Stored data (e.g. encrypted email, encrypted files, encrypted hard disks or volumes).
- Streamed data (e.g. encrypted chat, encrypted audio/video streams/calls, other encrypted traffic in transit[34]).

It is unclear who the proposed offence is directed at. It could be any of, a combination of, or all of the following:

- Persons under investigation for a specific crime or national security threat.
- Persons under arrest.
- Persons charged with a crime.
- Persons charged with a crime which meets a certain threshold of penalty units[35].
- Persons not under investigation, but who may have a relationship (either personal or professional) to a person who is under investigation, under arrest or is charged.
- Persons employed by a C/CSP or ISP which provides services to a person who is under investigation.
- Persons who are developing encryption or security software who are instructed to insert a backdoor for access by law enforcement.
- Persons not under investigation, arrest or charged who do not have any relationship with any person who is (i.e. the general public).
- Persons who are willing to assist in the decryption of data, either their own or those of others, but who are unable to comply for some reason (e.g. they no longer possess the secret/private key or know the password/passphrase).

Comments posted on the PGPNET[36] mailing list by a person going by the pseudonym 'MFPA', who resides in the UK where decryption assistance laws are in effect, sum up the issue rather well:

[34], SSL (http://en.wikipedia.org/wiki/SSL), TLS (http://en.wikipedia.org/wiki/Transport_Layer_Security), IPsec (http://en.wikipedia.org/wiki/IPsec), etc.

[35], If it is a crime which meets a certain threshold test, that threshold has not been specified.

[36] *PGPNET*, http://groups.yahoo.com/group/PGPNET/.

> "The warning given by police to anybody they arrest states quite clearly that the person does not have to say anything. Demanding that you (assist them to) decrypt is tantamount to demanding that you tell them something."

Currently under Australian law, as in the UK, the same rules apply with regards to investigation, arrest and being charged. A person has a right to the presumption of innocence and to defend themselves. This includes the right to refuse to comment or make a statement to law enforcement.

If the police believe an individual has committed a crime, it is the police's job to uncover evidence. Threatening a penalty for an administrative offence when the individual declines to provide information is only marginally more subtle than threatening violence when the individual declines to sign a confession.

Demanding that a person decrypt data places them in the position where they must reveal information in much the same way as forcing them to make a statement, which may be contrary to their interests, the right to defend themselves, their right to privacy, or any other reason that prompted the person to encrypt the data in the first place.

Oddly, the situation for those not charged with a crime may be different. Australian law currently provides for measures to compel witnesses to give evidence under certain circumstances, such as upon receipt of a subpoena to attend court. Furthermore, the right to refuse to answer on the grounds of possible self-incrimination is not always available (e.g. if the questioning is by a crime commission like the ICAC). If decryption on demand legislation were enacted targeting people who would be classed as a witness based on their possession of, or access to potentially incriminating encrypted data, then they may be compelled to decrypt that data. Compliance with such a demand may leave that person open to civil and/or criminal repercussions depending on the content or nature of the encrypted data and the circumstances under which the person had access to or possession of that encrypted data.

Those working for a C/CSP or ISP may be required under this legislation to deploy methods not only of intercepting communications data, but also of circumventing the encryption used by users of their C/CSP or ISP services. For stored data, such as encrypted email, it may not be possible to decrypt the data at all. For some streamed data, such as traffic between an end user and a secure website, it is possible, but this is commonly referred to as a Man-in-the-Middle attack[37][38]. Other streamed data, such as XMPP instant messaging with OTR encryption and ZRTP for VoIP services, have some defences against these types of attacks.

The purpose of encryption is to prevent any unauthorised party accessing information. There are numerous implementations of encryption and security software which are designed to prevent any type of interception, including providing protection against interception by an ISP or network operator. The resulting technical difficulties in decrypting data protected in this manner may result in any number of employees of a C/CSP or ISP open to being charged under this proposed legislation as a result of actions and technology that lies completely out of their control.

Those developing software and hardware security or encryption products may be required to insert backdoors to be used by law enforcement once certain requirements are met (e.g. a warrant is obtained against a user of such software or hardware). Inserting

[37] Benjamin D. McGinnes, *Cleaning A HTTPS Feed*, 2010, http://www.adversary.org/files/CleanFeedHTTPS-01.pdf.
[38] Wikipedia, *Man-in-the-Middle Attack*, https://en.wikipedia.org/wiki/Man-in-the-middle_attack.

backdoors is a dangerous practice as it is probable that third parties, such as criminals, may discover the backdoor and exploit it to the detriment of all users of those products. Meanwhile, products developed overseas will not contain these backdoors.

The result of introducing mandatory backdoors in Australian information security products would be twofold: firstly, it would leave users of those products vulnerable to having their confidential data exploited by unauthorised parties who have access to, or discover the backdoor; and secondly, it would result in a loss of business to foreign products which do not contain these backdoors.

Another possibility is that this legislation is non-discriminating. That is, it is directed at anyone in Australia, regardless of whether they are under investigation, under arrest, are charged, know someone who is, work for a C/CSP, work for an ISP, develop security products or none of these things. It is possible that the legislation is aimed at decryption on demand of any data at any time by order of any authorised law enforcement officer. If this is the case it opens up a host of issues. These include, but may not be limited to, any of the following: breaches of the privacy of citizens, abuse of this power to create a surveillance state, exposure of criminal or civil liability which would not otherwise occur without the decryption of data, abuse of this power by members of law enforcement and so forth.

An example of this power being utilised in a manner that could leave someone open to criminal liability would be: having an encrypted private diary which contained personal opinions which breached defamation[39] or other speech or expression related laws. The demand to decrypt this may result in the document being placed on the public record (e.g. as evidence) and the author charged, a result which would not have occurred had the diary been kept confidential.

An example of this power being used in a manner that could open someone to civil liability is if the encrypted data were commercial in-confidence or other confidential data. A demand to decrypt that data would necessitate a breach of a commercial agreement which may result in civil legal action, such as being sued. Furthermore the decrypted data may contain parts belonging to a third party, further increasing the arbitrary nature of the violation of privacy. Entering the decrypted data as evidence and therefore making it public may violate state or federal privacy regulations.

Regarding the potential for abuse of the power by law enforcement as Mr. Wayne Baffsky, a New South Wales barrister, recently said in relation to the overturning of a conviction under recently introduced New South Wales' consorting legislation:

> "I knew that was going to happen here, because you give anyone too much power and they're going to abuse it."[40]

That statement is true of more than just consorting legislation and could very easily be the case with the proposed decryption on demand legislation and other proposed national security legislation.

Finally, where a person wishes to comply with a decryption on demand order but they may be in a position where they are unable to do so. This inability may be the result of

[39] Electronic Frontiers Australia, *Defamation Laws & the Internet - Civil and Criminal Defamation*, Jan. 14, 2006, https://www.efa.org.au/Issues/Censor/defamation.html#civcrim.

[40] Stephen Jeffery, *'Give anyone too much power and they're going to abuse it': state's first consorting verdict overturned*, Aug. 14, 2012, http://www.smh.com.au/nsw/give-anyone-too-much-power-and-theyre-going-to-abuse-it-states-first-consorting-verdict-overturned-20120814-246a6.html.

not possessing, or no longer possessing, the secret information that is required to decrypt the data (e.g. not having, or no longer having, the private key and/or the password or passphrase required).

It would be possible for a third party to abuse this and frame someone. For example, by creating OpenPGP keys with that person's name and email address, encrypting data to that key and sending the data to that person anonymously, they could then tip off law enforcement that the person possesses serious incriminating evidence in an encrypted form. A variation would be to use old keys belonging to that person for which they no longer possess either the private key or passphrase for. As public keys cannot be deleted from the public key servers, there are many keys available which could be used to frame people who originally created them. One of the authors of this submission has at least two keys on the key servers in this state.

Without some legislative protection for people in this situation, the person may then be charged with failing to assist in the decryption of that data.

A special point needs to be made of one of the more common publicly available methods of cryptography: public key cryptography[41]. This is used for two main purposes: encrypting data and digitally signing data. This form of cryptography was effectively introduced[42] to the world by Phil Zimmermann with his Pretty Good Privacy (PGP)[43] software, originally written in the early 1990s. This has formed the basis of the OpenPGP[44][45] protocol; which is the standard followed by both PGP and the GNU Privacy Guard (GPG)[46][47] the two most common implementations. Public key cryptography is controlled by two-factor authentication: the private or secret key and a corresponding passphrase to unlock it. Possessing both the private key and the passphrase enables a person to decrypt data encrypted with that key and also to digitally sign data or messages.

If the proposed legislation in this section enabled law enforcement or the intelligence agencies to obtain copies of the private key(s) and passphrase(s) of anyone given a decryption on demand order, rather than decrypting the data and providing that decrypted data, it would place an unprecedented level of power in the hands of authorities. Not only would they be able to decrypt any data which has ever been encrypted with that key, including data which may be unrelated to the reason for which the order was given, they would then be able to sign messages or files using the person's key, effectively stealing their identity. In this manner, they could forge digital messages of an incriminating nature in the name of the person affected by the order. In conjunction with the power to add or remove data on a targeted computer, this could be used to frame someone through the manufacture of evidence.

Pirate Party Australia believes that this proposal reverses the traditional legal rights of accused people to refuse to incriminate themselves. We believe that it threatens the right of citizens to retain privacy in their personal affairs and information. Furthermore, professionals upon whom an onus is placed of protecting certain types of information,

[41] Wikipedia, *Public-key cryptography*, https://en.wikipedia.org/wiki/Public-key_cryptography.
[42] Wikipedia, *Public-key cryptography - History*, https://en.wikipedia.org/wiki/Public-key_cryptography#History.
[43] Wikipedia, *Pretty Good Privacy*, https://en.wikipedia.org/wiki/Pretty_Good_Privacy.
[44] OpenPGP, *About OpenPGP*, http://www.openpgp.org/about_openpgp/.
[45] IETF, *RFC4880: OpenPGP Message Format*, https://tools.ietf.org/html/rfc4880.
[46] GNU Privacy Guard, *GNU Privacy Guard*, http://www.gnupg.org/.
[47] Wikipedia, *GNU Privacy Guard*, https://en.wikipedia.org/wiki/GNU_Privacy_Guard.

such as lawyers protecting client information, doctors protecting patient records and journalists protecting sources, will be placed in jeopardy.

We believe that the proposal places an undue burden on employees of C/CSPs and ISPs to provide a level of assistance to authorities which may be beyond the scope or ability of their profession or expertise. Additionally, the proposal may require hardware and software developers to effectively sabotage their own business and livelihoods in order to comply.

b. Institute industry response timelines

Pirate Party Australia has no position on this item.

c. Mandatory data retention for 2 years.

This is a revival of the data retention plan which is modelled after previous European proposals, such as the Convention on Cybercrime[48] (of which Pirate Party Australia made a submission that recommended Australia does not accede to the convention[49]). It has been discussed with the ISP industry and pushed heavily by law enforcement during last year's Joint Select Committee hearing on the Cybercrime Legislation Amendment Bill 2011[50]. The request by law enforcement and intelligence organisations for data retention in the National Security Legislation Inquiry discussion paper goes well beyond the recommendations made a year ago in the Joint Select Committee's Review of the Cybercrime Legislation Amendment 2011.

Discussions relating the data retention plan have been held in camera between government and sections of the ICT industry. With the exception of submissions to the Joint Select Committee on Cyber-Safety's Inquiry into the Cybercrime Legislation Amendment Bill 2011 and the current Joint Parliamentary Committee on Intelligence and Security's Inquiry into potential reforms of National Security Legislation there has been no consultation with all the other stakeholders in this issue - the citizens of Australia.

As with the proposal to make failure to assist in decryption (C15a) an offence, there is very little in the PJCIS discussion paper regarding the specifics of this proposal. Nor is there any detail on the proposed data set, only that there is a data set. It does not specify, for example, whether that data set will be restricted to traffic data or content data. Though it is most likely that this proposal is only intended to target traffic data and not content data, we will address both of these possibilities, beginning with traffic data.

Traffic data is information about a communication such as the time it was sent, identifying information of the transmitting and receiving systems (e.g. IP addresses, DNS hostnames), the size of the transmission(s), the Internet protocol used and in many cases personally identifying information (e.g. an email address, an Instant Messaging (IM) address, a social network username, a VoIP number or address, etc). Traffic data is the limited amount of data used to ensure a communication is transmitted and received correctly and which may be logged by a system through which it passes.

---

[48] *Convention on Cybercrime*, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[49] Pirate Party Australia, *Submission to the Joint Standing Committee on Treaties regarding the proposed accession to the Council of Europe Convention on Cybercrime*, 2011, http://pirateparty.org.au/media/submissions/JSCOT%20CoE%20Cybercrime%20Convention.pdf.

[50] *Inquiry into Cybercrime Legislation Amendment Bill 2011*, 2011, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=jscc/cybercrime_bill/report.htm.

The majority of actual traffic data consists almost entirely of DNS look-ups and routing information. Previous government definitions, however, define traffic data as including any logged information for services they provide; such as mail server logs (which include the sender and recipient addresses) and include an assumption that HTTP proxy servers, which handle all web visits for Internet users, are still in use[51].

In order to retain data which would not ordinarily be (or is no longer) logged, an ISP would need to implement a scan (e.g. deep packet inspection) of all data transmitted through its' network. Methods to obtain data in this manner are identical to methods used to obtain specific content data or to perform an interception of data.

Even with cases where proxy servers are in use, users often utilise secure connections (e.g. HTTPS) for accessing content on sites such as ecommerce platforms, some of this personally identifying data may not be available to a C/CSP or ISP.

Traffic data could or would be linked with other personally identifying data, such as billing and account holder information held by the service provider through which it is sent. There are numerous issues pertaining to the retention of this data, both technical and legal, including some which overlap both realms.

Data retained under this policy would need to be stored in a secure manner which would be capable of preventing unauthorised access; either internally by employees of the company or organisation, or any external party (e.g. hackers, organised crime, foreign intelligence organisations, etc). Access controls would be required to prevent unauthorised access and to provide a thorough audit trail of all access to the system. Access controls and logging systems would need to be designed in a manner which prevents tampering with those logs in order to guarantee fidelity of those records.

The data would also need to be stored in a manner such that data no longer covered by the mandatory retention period (e.g. more than two years old) can be securely destroyed.

Data retention systems would need to include a system to search such a large data set for the specific information requested by a legally authorised party (e.g. ASIO or police). All searches would need to be logged by the access controls.

The entire data retention system would need to be securely backed up to prevent loss of any of the data set. This adds complexity beyond that norm of most backup systems. This includes, but may not be limited to, the following:

- Backups older than the mandatory retention period would need to be purged in a similar manner to that of the data retention system.
- The backups would need to be protected by similar access controls to the data retention system.
- A means of ensuring that backups could not be "restored" to another system by someone familiar with the system in order to
- freely access that data. Were that to occur they could retrieve any data, copy it and then wipe the system on which the backup had been restored to in order to conceal their actions.

[51], The majority of Australian ISPs ceased using or recommending the use of HTTP proxies during the transition from PSTN (dial-up) to ADSL connections around a decade ago.

- The amount of data retained, even when limited to traffic data, would be huge, even if compression and encryption were used when storing the data.

All of this data would need to be managed, stored and backed up within Australia. Outsourcing this role to offshore providers (e.g. cloud providers like Amazon) must not be permitted as once the data has left Australia, it would become subject to the laws of the country it was transferred to. Many countries, including the United States of America and the United Kingdom, have existing legislation (e.g. the United States' *USA PATRIOT Act* and the United Kingdom's *Regulation of Investigatory Powers Act 2000*) which could be used to access offshore backups of this data if it were transferred to those countries.

The costs associated with deploying such a comprehensive data retention system, including backup systems, would be considerable. It is likely that these costs would be passed on to consumers and businesses, which would result in a significant increase in Internet access fees.

The discussion paper refers to statistics regarding the number of C/CSPs, ISPs and other service providers in Australia, counting only ISPs with 1,000 customers or more. There is no indication as to whether these data retention requirements would be confined to C/CSPs and ISPs of that size or if it would extend to any business or organisation running any type of Internet based service. Nor does it address the issue of small to medium businesses or individuals who operate their own servers of various types (e.g. an email server, an IM chat server, a VoIP server and PABX, etc). This raises a number of questions:

- Will ISPs with less than 1,000 subscribers, small to medium sized businesses and individuals be required to retain their own data retention system? If so, will it require an external audit? If the system used does not comply with the requirements for a data retention system, will these organisations and individuals be subject to prosecution or forbidden from running their own servers?
- If these smaller organisations and individuals are not required to maintain their own data retention system(s), will their ISPs be required to monitor the traffic in order to log it? In order to implement such a scheme, the ISP would be required to intercept all traffic of their clients in order to obtain the specific types of data which they would normally be able to log on their own servers. Without a warrant this would be an unlawful interception.

The collection of all this data on every action performed by every individual and computer system in the country is indicative of a shift in focus by law enforcement and intelligence organisations from protecting the populace and the presumption of innocence to one of constant surveillance and suspicion of the populace. Where the existing targeted surveillance is akin to spear fishing, mandatory data retention is more like drift net fishing. The risk to individual privacy is enormous.

This data could be exploited in a number of ways. It would provide the opportunity for law enforcement and intelligence organisations to trawl through available data looking for something which might, on the surface, be of interest to them. Inappropriate or unlawful access to data by officials or employees of service providers could occur in much the same way as Victoria Police's Law Enforcement Assistance Program (LEAP)

database and other police resources which have been abused in the past[52][53][54][55], to the detriment of anyone in Australia. Even to the extent of resulting in homicide[56].

Analysis of the full data set could be used to map all connections and interactions of everyone in the country. Methods used to identify any criminal organisation or network could just as readily be applied to any group or organisation in the country. This could have a chilling effect on the exercise of individual rights and democratic participation. This type of analysis could then be exploited by law enforcement, intelligence organisations, elements within those organisations or other groups with which the analysis is shared to suppress organisations and groups which are not in and of themselves unlawful.

Content data is all the data within (each packet of) the actual communication; including what end users send and receive, as well as what has been identified as either actual traffic data or government definitions of traffic data. As described above, government definition of traffic data actually include a portion of actual content data.

As a result of the government definition of traffic data, their definition of content data consists of the data intentionally transmitted or received by end users such as the body of an email (including attachments), the text or files sent through IM, information uploaded to and downloaded from any web site, information sent and received through social networking sites, recordings of VoIP calls, etc. Some content data would be stored communications, such as email, while some of it is not generally stored and is merely transmitted between end user's computer systems and other computer systems.

All of the concerns regarding retention of traffic data apply to the retention of content data.

The definition of data which would need to be retained is a complete copy of all data transmitted in each direction across every data link in the country. This would by far exceed the storage capacity which would be required for traffic data and beyond the technical feasibility of most organisations in this country. The associated costs, which would be passed on to businesses and consumers, would be crippling.

Additionally, mandatory retention of content data is effectively the equivalent of mandatory interception of all communications in the country. This would be a massive invasion of everyone's privacy all of the time.

Unauthorised or inappropriate access to specific communication (e.g. email, IM chat transcripts, social media content, etc) would be both an abuse of power held by authorities and service providers with the potential to lead to further abuses of power. Content obtained through this level of surveillance could be used to expand analysis of any network or group in the country, as described in relation to traffic data analysis, to a significant extent.

[52] Cameron Houston, *Leak fears as 80 police access file on St Kilda teen*, Mar. 6, 2011, http://www.theage.com.au/victoria/leak-fears-as-80-police-access-file-on-st-kilda-teen-20110305-1biyq.html.

[53] Ry Crozier, *Vic Police probes illicit database access*, Mar. 7, 2011, http://www.itnews.com.au/News/250321,vic-police-probes-illicit-database-access.aspx.

[54] Ry Crozier, *Victoria Police delay crime database swap*, Mar. 29, 2010, http://www.itnews.com.au/News/170746,victoria-police-delay-crime-database-swap.aspx.

[55] Victoria Police, *Making the leap to LINK*, Mar. 18, 2009, http://www.police.vic.gov.au/content.asp?Document_ID=20195.

[56] Wikipedia, *Murders of Terrence and Christine Hodson*, https://en.wikipedia.org/wiki/Murders_of_Terrence_and_Christine_Hodson.

Furthermore, protocols which encrypt communication by default, in many cases without the knowledge or active engagement of the end user, could be used in conjunction with the proposed decryption on demand legislation to criminalise anyone in Australia at any time.

Since the adoption of legislation in Europe by European Union countries to conform to the *Convention on Cybercrime*, a number of those countries have since reversed their position on data retention. Germany in particular has rejected data retention as being in breach of its constitution. The following is taken from the Arbeitskreis Vorratsdatenspeicherung (German Working Group on Data Retention) report into the effectiveness of data retention as an investigative tool during the period in which data retention was in effect in Germany:

> ”Blanket data retention can actually have a negative effect on the investigation of criminal acts. In order to avoid the recording of sensitive personal information under a blanket data retention scheme, citizens increasingly resort to Internet cafés, wireless Internet access points, anonymization services, public telephones, unregistered mobile telephone cards, non-electronic communications channels and such like. This avoidance behaviour can not only render retained data meaningless but even frustrate targeted investigation techniques (e.g. wiretaps) that would possibly have been of use to law enforcement in the absence of data retention. Because of this counterproductive effect, the usefulness of retained communications data in some investigation procedures does not imply that data retention makes the prosecution of serious crime more effective overall. All in all, blanket data retention can actually be detrimental to the investigation of serious crime, facilitating some investigations, but frustrating many more.”[57]

It is likely that implementing data retention in Australia would have similar effects to those observed in Germany. The effect would not be to prevent organised crime or terrorism; it would merely result in greater concerted effort by organised criminals and terrorists to conceal their activities and communication. Meanwhile, the privacy and security of innocent, law abiding citizens would certainly be threatened and probably breached.

Pirate Party Australia believes that data retention, of either traffic data or content data, is a gross assault on the basic right to privacy of everyone in Australia. We believe that data retention is not an effective tool in fighting crime or terrorism and urge the government to reject this proposal.

Telecommunications Act 1997

16. Amending the Telecommunications Act to address security and resilience risks posed to the telecommunications sector. This would be achieved by:

a. By instituting obligations on the Australian telecommunications industry to protect their networks from unauthorised interference

[57] Arbeitskreis Vorratsdatenspeicherung, *Serious criminal offences, as defined in sect. 100a StPO, in Germany according to police crime statistics*, http://www.vorratsdatenspeicherung.de/images/data_retention_effectiveness_report_2011-01-26.pdf.

This proposal is worthy of support. Pirate Party Australia also recommends a provision requiring ISPs and other companies operating online to be required to warn their customers and the general public of any data breaches. This would enable their customers to take immediate action to change and secure their private data. This in turn would minimise the window for such privacy breaches to be able to cause financial or other harm to the customers of a company whose security has been breached.

b. By instituting obligations to provide Government with information on significant business and procurement decisions and network designs

This is reasonable as part of any security assessment of the telecommunications industry. Any attempt to mandate specific systems would be a serious imposition on a company. We believe the best approach would be to mandate security standards, but not how these security requirements be met.

c. Creating targeted powers for Government to mitigate and remediate security risks with the costs to be borne by providers

Any provision granting the Government powers to alter security systems to mitigate risks must be limited to only the most extreme cases where the telecommunications provider has acted negligently in securing their systems and has either refused or has shown a clear inability to adequately address the problem. In such cases it is reasonable that any cost be borne by the provider.

d. Creating appropriate enforcement powers and pecuniary penalties

Pirate Party Australia does not have a position on this.

Australian Security Intelligence Organisation Act 1979

17. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions by:

a. Using third party computers and communications in transit to access a target computer under a computer access warrant.

As the discussion paper itself notes, "that using a communication in transit or a third party computer may have privacy implications, appropriate safeguards and accountability mechanisms would need to be incorporated into such a scheme."[58]

This is an understatement, to say the very least. Granting power of this nature could very easily be combined with other sections in the following manner:

- With B11c to deliver Trojans/malware to be planted on targeted systems.
- With B11c to launch attacks on targeted systems.
- With B11c and C15a to plant encrypted data which a person is unable to decrypt and is then charged for.
- With B11c and C15c to create a false trail for data retention.

[58] Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats Discussion Paper*, 2012, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/additional/discussion%20paper.pdf.

There may be other ways this type of power might be used to the detriment of the privacy of Australians and this must be stringently guarded against.

b. Clarifying that the incidental power in the search warrant provision authorises access to third party premises to execute a warrant

This proposal can raise serious concerns for the third party, whose premises would be accessed under this provision. Accessing a third party's premises would require the cooperation of the occupant, or it would pose serious risks for their privacy, safety and property. It does not satisfy the requirement that a legal invasion of one's privacy not be arbitrary. Breaking doors or computer security systems of innocent third parties to access information about a suspect subjects exposes the third party to undue risk. Where such powers are deployed, it must be necessary to proceed only with the cooperation of the third party.

c. Clarifying that reasonable force may be used at any time during the execution of a warrant, not just on entry.

If this is just an administrative change to update the headings of "Authorisation of entry measures" to reflect the use of *existing* powers beyond the point of entry to a location specified in the warrant, then Pirate Party Australia has no problem with such a clerical update.

That said, the discussion paper has been unclear on a number of matters already and it is unclear just what powers this proposal is authorising. If this power specifically applies to the reasonable force necessary to apprehend a suspect at any time during the execution of a warrant, i.e. if sufficient evidence was uncovered during a search to make an arrest, this seems to be a reasonable adjustment.

If, however, reasonable force could be employed to recover encryption keys, statements or allows any form of coercion of a suspect, this would be tantamount to torture and represent a serious erosion of protections granted to Australian citizens under the law.

d. Introducing an evidentiary certificate regime.

Allowing the use of evidentiary certificates to protect the identity of an officer from the court should be flatly rejected. This is a troubling proposal which weakens the ability of a defendant to receive a fair trial. A representative of an officer would not be capable of providing adequate answers under cross-examination.

Part of any testimony in a court of law is the credulity of the witness. Having a surrogate to speak on behalf of an officer would protect the officer from direct scrutiny, weakening the court's ability to assess the credibility of the officers claims.

We recommend that where this power already exists that it be repealed. Any evidence given through such a system must be considered considerably weaker than any testimony given directly by the officer. Where an officer's identity must be kept secret (e.g. in accordance with section 92 of the ASIO Act, or to protect the identity of other undercover operatives or informants), there are existing judicial safeguards which are already sufficient to the task of protecting the officer's or informant's identity and retaining operational security.

Intelligence Services Act 2001

Amending the Intelligence Services Act to:

a. Add a new ministerial authorisation ground where the Minister is satisfied that a person is, or is likely to be, involved in intelligence or counter-intelligence activities.

This seems to be a reasonable adjustment of the legislation so long as all the proposed safeguards are imposed. Most importantly, the provision subjecting any investigation to the usual stringent warrant tests must be included. We suggest that a time period ought to be put in place, after which a judicial review would evaluate the ministerial decision and either ratify or overturn it.

b. Enable the Minister of an Agency under the IS Act to authorise specified activities which may involve producing intelligence on an Australian person or persons where the Agency is cooperating with ASIO in the performance of an ASIO function pursuant to a section 13A arrangement. A Ministerial Authorisation will not replace the need to obtain a warrant where one is currently required.

This is an acceptable proposal only if all of the limitations put forward in the discussion paper are adhered to and judicial oversight is required. As mentioned above, the judiciary is the most appropriate body to have the authority to order investigations. Empowering the Attorney-General with such authority risks Australia's intelligence services being deployed for political reasons. A proper separation between judiciary and government must be maintained at all times.

c. Enable ASIS to provide training in self-defence and the use of weapons to a person cooperating with ASIS.

Like much of the discussion paper, this section is vague. If weapons and self-defence training was limited to Commonwealth, State and Territory bodies that already have the legislative right to carry arms, as alluded to in the discussion paper, this is a reasonable amendment.

However the following paragraph granting powers to the Foreign Minister to approve foreign bodies for the provision of training is deeply concerning. This could be used to train insurgent armies, assassination squads and even terrorists. Such activities are not justified under any circumstances and is contrary to Australia's national interest. Any tool created to fight foreign enemies can be turned upon the Australian people or at minimum be justification for our enemies to adopt the same strategies against us.

The folly of such programs is starkly evident as a similar operation carried out by the USA in the 1980s has led directly to the War on Terror. US Secretary of State, Hillary Clinton pointed this out when she said:

> *"Part of what we are fighting against right now, the United States created. We created the Mujahideen force against the Soviet Union (in Afghanistan). We trained them, we equipped them, we funded them, including somebody named Osama bin Laden. And it didn't work out so well for us."*[59]

[59] *Interview With Cynthia McFadden of ABC's Nightline*, Nov. 7, 2010, http://usrsaustralia.state.gov/us-oz/2010/11/07/ds8.html.