Submission to the Senate Legal and Constitutional Affairs References Committee Comprehensive Revision of the *Telecommunications (Interception and Access) Act 1979*

Pirate Party Australia

Simon Frew (simon.frew@pirateparty.org.au)
Mozart Olbrycht-Palmer (mozart.palmer@pirateparty.org.au)

27 February 2014

Contents

Introduction

Pirate Party Australia would like to thank the Senate Legal and Constitutional Affairs Committee for the opportunity to submit on the important issue of reform of the *Telecommunications (Interception and Access) Act 1979*. Recent revelations surrounding the extent of intrusive surveillance in a digital context have highlighted the issue in the public consciousness, and the Pirate Party is very pleased to see such a comprehensive review.

The Pirate Party proposes a radical approach to reforming the *Telecommunications (Interception and Access) Act 1979* that requires its complete replacement with modern legislation compatible with the digital age and built around a focus of protecting privacy, allowing open public discourse on the extent of communications interception, safeguards against abuse, and the provision of judicial oversight.

About Pirate Party Australia

Pirate Party Australia is a political party registered under the *Commonwealth Electoral Act 1918*. The Party was founded in late 2008, and contested its first Federal Election in 2013. The Party's main areas of concern are intellectual property rights reform, privacy rights, increased governmental transparency, and opposition to censorship.

Pirate Party Australia is a member of a worldwide movement that began in Sweden in 2006, and has since spread to more than 40 different countries. Pirate Parties have been elected to all levels government — local, state, national and supranational — with 45 state seats in Germany, three seats in the Icelandic Parliament, and two Members of the European Parliament.

1 Abbreviations

LEIA Law enforcement and intelligence agency.
TIA Act *Telecommunications (Interception and Access) Act 1979*.

2 The TIA Act at present

The nature of telecommunications has fundamentally changed since the TIA Act was enacted in 1979. There have been many amendments

made to attempt to keep the legislation up to date, resulting in legislation that is over-complicated and does not adequately reflect the values of Australian society. A recent poll by Essential Research indicated that 80% of the population disapproves of warrantless access of communications by LEIAs.[1]

Despite varying opinions of those who leak secret information relating to interception and access (and surveillance more broadly) — for example, Senator Scott Ludlam considers Edward Snowden in high regard, while Attorney-General Senator George Brandis considers Snowden a traitor[2] — the reality is that the leaks provided have helped to open public discussion and debate over what sorts of powers are appropriate for LEIAs, and revealed the extent of surveillance and surveillance powers within the 'Five Eyes' nations (Australia, Canada, New Zealand, the United Kingdom and the United States).

There is an apparent disconnect between:

1. The understanding of the powers granted to LEIAs by legislation,
2. The interpretation of those powers by LEIAs,
3. The extent of the use of those powers, and
4. The public perception of what those powers are and how they should be used.

Ideally all of these should be in agreement. However, years of assumption that the public should be unaware of the nature of surveillance powers and the way they are being used has led to the current discrepancy.

Legislation relating to telecommunications interception and access is currently unclear when it comes to providing an easily understandable framework for surveillance operations. The public must be aware of exactly which powers are granted to LEIAs, and how the provisions granting those powers are being interpreted. Ideally there would be minimal scope for confusion between what the legislation allows, and what it has been interpreted to allow. The public must also be aware of the boundaries of those powers, and the rights they have available to protect their privacy from abusive intrusion, as well as any remedies available against overuse of LEIA powers. At the moment, it is clear this is not the case, and it is also clear that the public is not being adequately consulted over what powers should exist and how they should be used.

Pirate Party Australia believes that the best way to address shortcomings in the TIA Act is to repeal the current legislation and adopt

[1] Essential Research, *the Essential Report*, 18 February 2014, http://essentialvision.com.au/documents/essential_report_140218.pdf

[2] Commonwealth, *Parliamentary Debates*, Senate, 11 February 2014, page 20 (George Brandis).

new laws that are clear, relevant to modern technology, and provide adequate privacy protections for Australian citizens.

3 Replacing the TIA Act

The TIA Act is more than 30 years old, and was enacted in the pre-Internet era. It is clear that legislation that does not anticipate technological change soon becomes outdated and used in ways that they were not intended to be used, or ways that are unacceptably broad. Another consideration is social change, and that was appropriate in the past is often no longer appropriate for a modern society.

A related example is section 313 of the *Telecommunications Act 1997*, which has been used by Australian Security & Investments Commission (ASIC) and other government departments to compel Internet service providers (ISPs) to block access to websites. Section 313 was originally intended to promote cooperation between telecommunications providers and law enforcement agencies: it was never meant to be used as a tool of censorship in the hands of Government regulators, regardless of whether the censorship is noble or not. The fallout from heavy-handed use of section 313 can be seen when ASIC's attempt to thwart scams resulted in the blocking of 250,000 websites, including among them Melbourne Free University. According to the Sydney Morning Herald:

> ASIC made the concession in a statement at a senate estimates hearing on Tuesday night, after it caused controversy by interpreting a 15-year-old law in the Telecommunications Act as giving it the ability to block websites.
>
> ASIC asked internet service providers (ISPs) to block sites it believed were defrauding Australians by IP address (such as 203.56.34.11) instead of domain name (such as sitedefraudingaustralians.com). This meant thousands of other sites were blocked in the process, as many sites are often hosted on one shared IP address.
>
> ASIC told senate estimates in its opening statement that it was now examining how it could ensure only a site's specific domain name was blocked …
>
> Use of section 313 to block websites was only uncovered last month after the webmasters of the Melbourne Free University

site couldn't figure out why it was no longer accessible.[3]

This is also relevant to the previous section, as it illustrates the disconnect between understandings of powers relating to telecommunications in Australia.

Much the same risk is posed by retaining the TIA Act or attempting to amend it to adapt to a fundamentally different paradigm. The legislation has been amended several times in the last fifteen years, and while there is obviously need to maintain modernity in legislation through amendment, Pirate Party Australia believes that such amendments preserve a fundamentally inappropriate approach to telecommunications interception and access.

In short: the *Telecommunications (Interception and Access) Act 1979* is founded on an approach that is no longer suitable for contemporary Australia, and no amount of amendment will be able to resolve the fundamental disconnect between the Act as it stands and the needs and values of the Australian community.

4 Restricting powers by default

There has been a tendency towards a form of regulatory capture whereby those charged with regulating LEIAs become advocates for or defenders of the retention and expansion of the powers of those agencies. The Attorney-General's Department has in the past argued on behalf of LEIAs rather than take an impartial view — that is, the Department has advocated that LEIA powers be expanded, including when providing evidence to inquiries on the matter.[4]

This is not an ideal situation, as it indicates that government positions are based on the views of the agencies it is meant to regulate and not on an examination of the balanced needs of the community as determined by a wealth of independent evidence. They are not representing the interests of the electorate by doing so. The result is that, in Pirate Party Australia's view, the ability for LEIAs to intercept and access communications is geared more towards the efficient operation of agencies and less towards safeguards against privacy intrusions.

[3]Ben Grubb, 'How ASIC's attempt to block one website took down 250,000', *Sydney Morning Herald* (online), 5 June 2013, http://www.smh.com.au/technology/technology-news/how-asics-attempt-to-block-one-website-took-down-250000-20130605-2np6v.html

[4]Attorney-General's Department, Submissions 218 and 235 to the Joint Parliamentary Committee on Intelligence and Security, *Inquiry into potential reforms of National Security Legislation*, 2012, http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/subs.htm

Telecommunications interception and access legislation should be firmly grounded in ensuring that minimal access to personal information is available by default. In many ways a technocratic approach to efficiency in the legal system has led to situations where processes are expedited when they should not be. The default position of LEIAs in relation to interception and access should be no power without judicial oversight.

There should be effort involved in obtaining authority for intercepting and/or accessing communications. All activities requiring the interception and/or access of communications must require a legal process such as an application for a warrant. There should be no ability for law enforcement or intelligence officers and agencies to intercept or access communications without such a process.

5 Clarity and clear lines of authority

When dealing with personal information and intrusions of privacy, legislation must be absolutely clear in terms of what it permits, the powers it confers, and the protections it provides. This is an area of law where flexibility should be kept to a minimum, and the requirement for interpretation reduced as much as possible. Reform of the TIA Act must take into account the need for clarity with regard to the issues raised.

Society has an interest in providing LEIAs with the tools and powers necessary to adequately enforce the law, prevent threats to our national security and investigate crime. Society also has an interest in protecting the privacy of citizens and ensuring that personal information is not abused.

To this end, law enforcement and intelligence officers must know what their powers are, what degree of authorisation they need, and what regulations they must adhere to when intercepting and accessing data. Likewise, citizens must be able to know the limits of LEIA powers in order prevent abuse.

A replacement TIA Act that provides clarity on these powers, obligations, rights and responsibilities is necessary to build confidence, efficiency and fairness into the interception and access procedures, to protect both citizens and law enforcement and intelligence officers.

6 Guiding principles for a new act

6.1 Principle: protecting privacy

Privacy is a fundamental aspect of living in a democratic society. People need the personal space to explore new ideas, express and develop their views and opinions and carry on their personal lives without the fear that they are under surveillance. The right to privacy is under persistent threat as technology makes the proliferation, collection and analysis of personal data easier than ever before.

The law is trailing behind technology and LEIAs are pushing for greater access to private information. Politicians — through a combination of technological illiteracy, and wanting to appear tough on crime and promoting national security — have largely approved expansion of electronic surveillance. Although modern technologies enable greater surveillance of the population, this does not mean that it is a good idea to do so. Such measures fundamentally change the nature of democracy. According to a study by the European Parliament Directorate-General for Internal Policies, the tensions between national security and citizens' privacy can become a threat to democracy itself.[5]

In light of the revelations that the US National Security Agency (NSA) is (or at least was) running a global surveillance regime with the assistance of the Australian Signals Directorate (ASD), it is clear that citizens' privacy has been compromised without any public knowledge, discussion and debate.[6] While this is a global problem, the ASD is an integral part of the 'Five Eyes' programme and as such must be reigned in to conform to expected community standards.

LEIAs have become increasingly reliant on warrantless access to so-called 'metadata' or 'telecommunications data' in their investigations. Contrary to assurances from supporters of warrantless surveillance, metadata *is* private information. It includes who communicated with whom, times of communications, email titles, locational data, and so on, all of which can be compiled to make a detailed record of the movements of and relationships between private citizens without establishing reasonable suspicion that criminal activity is actually taking place.

In the *Telecommunications (Interception and Access) Act 1979 Annual Report 2012–13* there were 312,929 cases of access to citizens' data

[5]European Parliament Directorate-General for Internal Policies, *National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law*, 2013, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf

[6]Ibid.

being authorised without a warrant.[7] While this may be a useful tool for law enforcement, it amounts to an enormous privacy invasion for those whose data is accessed.

Pirate Party Australia believes that the balance between civil liberties and LEIA powers has shifted too far in favour of the latter, and judicial oversight needs to be imposed on access to the records of private citizens in order to help restore the balance.

6.2 Principle: targeted surveillance

Related to the principle of protecting privacy is that of targeted surveillance. The Pirate Party recommends reform of the TIA Act mandate that surveillance must focus only on specific individuals and/or organisations that are suspected of criminal activity and prohibit the indiscriminate interception and access of data.

Article 17 of the International Covenant on Civil and Political Rights provides:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

Similarly, Article 12 of the Universal Declaration of Human Rights states much the same:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Treating all citizens essentially as suspects without due cause is arbitrary precisely because there is no reason other than perceived improvement in the efficacy of policing. It infringes upon the privacy of individuals who are not involved in criminal activity and/or are of no interest to LEIAs. Pirate Party Australia believes that indiscriminate surveillance is in violation of international law on this basis.

International experience provides a strong case for avoiding blanket interception and access of personal information. In Germany a poll by Forsa indicated that mandatory data retention — that is, the interception and storage of all communications data — caused half the

[7] Attorney-General's Department, *Telecommunications (Interception and Access) Act 1979 Annual Report 2012–13*, 2013, http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/TSLB-GAPSTIAActAnnualReport2012-13.doc (page 42)

population to avoid using the phone and Internet to contact psychotherapists or marriage counsellors.[8]

According to the European Digital Rights *Shadow evaluation report on the Data Retention Directive (2006/24/EC)*:

> With a blanket and indiscriminate telecommunications data retention regime in place, sensitive information about social contacts (including business contacts), movements and the private lives (e.g. contacts with physicians, lawyers, workers councils, psychologists, helplines, etc.) of 500 million Europeans is collected in the absence of any suspicion.[9]

A situation that allows law enforcement and intelligence agencies to indiscriminately intercept and access data — regardless of how many or how few are affected — is not healthy for a free and democratic society to thrive. It should not be that citizens are treated by the system as suspects by default, regardless of whether that is the intention of the legislature. Good intentions can still lead to negative results.

Although data retention in Australia is not yet mandatory, it would be wise to seek a prohibition on the practice (aside from retention necessary for the operation of telecommunications services). The case against data retention is supported by declarations of unconstitutionality (for breaching the right to privacy, and private communications) in Germany[10] and Romania.[11] Although Australia lacks the constitutional protections of these and other countries, it is clear that data retention is a significant risk to privacy and impacts on human rights. Pirate Party Australia acknowledges that the previous government shelved data retention proposal, and the Party believes that such proposals should remain shelved.

On the other hand, there is still the threat of 'collateral damage' when it comes to the mass interception and access of data. Intercepting and accessing the communications of an entire building, for example, runs the risk of capturing information outside the scope of an investigation. Consider a sharehouse situation where several people may be sharing

[8] Forsa, *Meinungen der Bundesbürger zur Vorratsdatenspeicherung* [*Opinions of German Citizens on Data Retention*], 2008, http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf (in German), cited in European Digital Rights, *Shadow evaluation report on the Data Retention Directive (2006/24/EC)*, 2011, http://www.edri.org/files/shadow_drd_report_110417.pdf

[9] European Digital Rights, *Shadow evaluation report on the Data Retention Directive (2006/24/EC)*, 2011, http://www.edri.org/files/shadow_drd_report_110417.pdf

[10] BBC News, 'German court orders stored telecoms data deletion,' 2 March 2010, http://news.bbc.co.uk/2/hi/europe/8545772.stm

[11] Constitutional Court of Romania, Decision no. 1258, 8 October 2009, http://www.legi-internet.ro/fileadmin/editor_folder/pdf/Decizie_curtea_constitutionala_pastrarea_datelor_de_trafic.pdf (in Romanian).

the same Internet connection or landline telephone, and one of those is under surveillance. Intercepting and/or accessing the communications of that house in order to investigate the sole suspect will capture communications of uninvolved third parties (both the other tenants and those they communicate with).

This is a regrettable situation, however Pirate Party Australia accepts that there may be some necessity for privacy intrusions where the communications of a suspect cannot be reasonably differentiated from others. This is why the Pirate Party supports targeted surveillance that identifies suspects and reduces the risk of capturing third party communications. The Party addresses warrants and judicial oversight later in this submission, but a guiding principle for reform of the TIA Act must be to have clear distinction as to who the target of surveillance is, and require that an assessment of the risk to the personal privacy and information of unrelated persons be made.

It must be clear that interception and access of communications by LEIAs must only be conducted with regard to clearly identifiable individuals and sources. There should be no scope to expand communications beyond those identified in a warrant, and strong efforts should be made to reduce the interception and access of communications that are outside the warrant.

6.3 Principle: transparent operation

For the most part, the current system operates with an acceptable amount of transparency. Pirate Party Australia supports the continued publication of statistics relating to requests for interception and access by LEIAs in Australia.

Transparent operation does not necessarily mean the complete disclosure of operational information. However, publication of statistics and compliance statements would be appropriate. Pirate Party Australia views the following minimum requirements as positive ways to ensure the ongoing transparent operation of the telecommunications interception and access regime in Australia. These are based on an assumption that interception and access occurs within a warrant-only system with no warrantless interception or access.

Pirate Party Australia advocates the quarterly and annual publication of:

- The number of warrants for interception and access requested,
- The number of warrants for interception and access granted,
- The number of times interception and access powers are used,

- The shortest and longest periods that interception and/or access warrants have been used,
- The average duration over which interception and access occurs,
- The number of successful convictions as a result of using telecommunications interception and access powers,
- Statistics for the types of interception and access — whether targeted towards a specific person or telecommunications connection, etc,
- The number of individuals and/or organisations inadvertently affected by interception and access, and
- Which law enforcement and intelligence agencies, including government departments, commissions, regulators and so on, make requests for interception and access and how many are made by those organisations.

Under a telecommunications interception and access regime that allows for warrantless interception and access, the above should include statistics on the use of warrantless powers.

It would be inappropriate for LEIAs and government departments to provide complete details on the security systems used to prevent unauthorised access to data that they may be collecting and storing, but this does not mean they should go without scrutiny. Pirate Party Australia advocates the development of government-wide standards for data storage to protect privacy, which should be made publicly available. Such standards should embody current best practice for data security and be available for public and industry scrutiny. This should in effect mean that the executive is guaranteeing Australian citizens that data security in interception and access scenarios meets minimum modern standards. Employing such a mechanism would help reduce privacy concerns and concerns surrounding potential abuse of personal information.

6.4 Principle: judicial oversight and warrants

Pirate Party Australia opposes any interception and/or access of communications without a warrant. As mentioned above, a recent opinion poll by Essential Research demonstrated that 80% of the representative sample polled are opposed to warrantless surveillance by both law enforcement and intelligence agencies.[12] With such widespread opposition, any government wishing to reflect the values of society must wind back surveillance powers.

[12]Essential Research, *the Essential Report*, 18 February 2014, http://essentialvision.com.au/documents/essential_report_140218.pdf

There must be an independent judicial assessment of the probability that the interception and/or access of an individual or group's communications would result in the successful prevention of a crime or apprehension of a suspect. As with bail applications and apprehended violence orders, this must consider the threat that may be posed by the individual (or those with whom they are communicating) to society, and weigh up the risk to the target's privacy against the gain to society.

Where there is insufficient evidence to justify intrusion into a person's privacy, no warrant should be issued. As mentioned earlier, both Article 17 of the International Covenant on Civil and Political Rights and Article 12 of the Universal Declaration of Human Rights provide a right against arbitrary interference with privacy. One of the simplest ways to prevent arbitrary interference with privacy is to require independent assessment of the benefit of telecommunications interception and access in the form of judicial oversight and the warrant system. This would allow an independent member of the judiciary to consider the risks, providing both the targets and the officers with safeguards that protect them from undue intrusions of privacy and allegations of abuse respectively.

Pirate Party Australia advocates this approach to reform.

6.5 Principle: safeguards against abuse

Any system dealing with private and personal information must have in-built legislative safeguards against the abuse of that data. Data collected for one reason must only be used for the intended purpose and not become the source for so-called fishing expeditions. Such methods can be used to circumvent privacy protections and any loophole allowing such breaches must be closed.

One simple safeguard for ensuring that intercepted communications are not abused is to ensure that information collected is permanently destroyed following the end of an investigation or when it is assessed as being of no use to an investigation. Data that has been erroneously collected or is deemed irrelevant should not be stored for any longer than is necessary, for several reasons. As unfortunate as it is, corruption remains a risk even in a developed democracy such as Australia, and Australians need to be confident that their data, if collected, is not accessed without authorisation. Destroying data in a timely fashion would help alleviate concerns. A second concern is that centralised storage of large quantities of data presents a high value target for domestic and foreign actors, both state and non-state. We should be cautious about presenting a treasure trove of intelligence information to foreign intelligence agencies or individuals with unscrupulous motives. A third concern is that stored data could be used to intimidate

suspects and witnesses in the future, or be used as circumstantial evidence to accuse or discredit individuals via fishing expeditions.

Strong safeguards must exist to protect collected data and citizens' privacy.