Electronic Frontiers AUSTRALIA 20 YEARS

PO Box 1302, Kensington VIC 3031
W www.efa.org.au T +61 3 9013 9492
E email@efa.org.au F +61 3 9013 9468
@efa_oz

Committee Secretary
Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House, Canberra ACT 2600

Via email to: legcon.sen@aph.gov.au

3rd March 2014

Dear Committee Secretary,

Re: Comprehensive revision of Telecommunications (Interception and Access) Act 1979

EFA welcomes the opportunity to provide input into this review. Please find our submission on the following pages. Please do not hesitate to contact me should you require any further information.

About EFA

Established in January 1994, Electronic Frontiers Australia, Inc. (EFA) is a national, membership-based non-profit organisation representing Internet users concerned with on-line freedoms and rights.

EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting online civil liberties. EFA members and supporters come from all parts of Australia and from diverse backgrounds.

Our major objectives are to protect and promote the civil liberties of users of computer based communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political and civil liberties issues involved in the use of computer based communications systems.

Yours sincerely,

Jon Lawrence
Executive Officer

Electronic Frontiers AUSTRALIA 20 YEARS

Submission to the comprehensive revision of the Telecommunications (Interception and Access) Act 1979

EFA understands the challenges that Australia's intelligence and law enforcement agencies face in the context of increasingly digitised communications.

Recently, a number of whistleblowers have exposed ongoing abuses of individual privacy by the United States' National Security Agency and its allied agencies. These leaks have catalysed debate over the effectiveness of existing laws governing privacy and telecommunications interception, and their relationship with national security. In light of the attention surrounding these issues, EFA believes that Australia's laws governing these issues are now in need of urgent revision.

EFA supports the appropriate and reasonable reform of relevant legislation to ensure that Australia's intelligence and law enforcement agencies are equipped to detect, investigate and prosecute serious criminal activity, without compromising the privacy and civil liberties of Australian citizens and residents.

EFA is however seriously concerned that revision of the **Telecommunications (Interception and Access) Act 1979** must balance ensuring national security with protecting individual rights. In brief, we propose that any reform to the Telecommunications (Interception and Access) Act 1979 must include strong privacy protections for Individuals and accountability provisions for government, security, law enforcement, and associated agencies.

This submission recommends changes to the current Telecommunications (Interception and Access) Act 1979, specifically with regard to:

> *(a) the recommendations of the Australian Law Reform Commission For Your Information: Australian Privacy Law and Practice report, dated May 2008, particularly recommendation 71.2; and,*
>
> *(b) recommendations relating to the Act from the Parliamentary Joint Committee on Intelligence and Security Inquiry into the potential reforms of Australia's National Security Legislation report, dated May 2013.*

Each point is addressed separately with points of concern identified by EFA in relation to privacy and security of information of Australian citizens. These sections are identified as:

1. Australian Privacy Law and Practice report, dated May 2008; and,
2. Australia's National Security Legislation report, dated May 2013.

Within these sections are highlighted areas identified as concerns by EFA followed by recommendations for changes to the specific sections of the ACTs (identified above). This is then followed by a conclusion and a summary of the recommendations identified within this submission.

1. Australian Privacy Law and Practice report, dated May 2008

Within this section only the areas of the Act that are of most concern to the EFA are identified and addressed, including recommendations for changes to the Act.

Section 5 of the *Australian Privacy Law and Practice Report* (2005) provides recommendations that should be adapted for the *Telecommunications (Interception and Access) Act 1979*. These recommendations are identified below followed by EFA amendments for inclusion or otherwise, into the *Telecommunications (Interception and Access) Act 1979*.

Recommendation

This recommendation supports and adds to the recommendations from the ALRC review, which are addressed individually below:

> ***ALRC Recommendation 5–1*** *The regulation-making power in the Privacy Act should be amended to provide that the Governor-General may make regulations, consistent with the Act, modifying the operation of the model Unified Privacy Principles (UPPs) to impose different or more specific requirements, including imposing more or less stringent requirements, on agencies and organisations than are provided for in the UPPs.*

a) Changes to Part 2-1 section 7(1):

Changes to include: (1A) the Governor-General may make regulations, consistent with the Act:

> (a) modifying the operation of the model Unified Privacy Principles (UPPs), and/or
>
> (b) impose different or more specific requirements, including imposing more or less stringent requirements than are provided for in the UPPs, on
>
> > (i) agencies, and
> >
> > (ii) organisations.

b) Changes to Part 3-1 section 107G:

Changes to include: (3) Reference to the Unified Privacy Principles (UUP) model prior to

ALRC Recommendation 5–2 *The Privacy Act should be redrafted to achieve greater logical consistency, simplicity and clarity.*

> ***ALRC Recommendation 5–3*** *The Privacy Act should be renamed the Privacy and Personal Information Act. If the Privacy Act is amended to incorporate a cause of action for invasion of privacy, however, the name of the Act should remain the same.*
>
> ***ALRC Recommendation 5–4*** *The Privacy Act should be amended to include an objects clause. The objects of the Act should be specified to:*
>
> > *(a) implement, in part, Australia's obligations at international law in relation to privacy;*
> >
> > *(b) recognise that individuals have a right to privacy and to promote the protection of that right;*

(c) recognise that the right to privacy is not absolute and to provide a framework within which to balance that right with other human rights and to balance the public interest in protecting the privacy of individuals with other public interests;

(d) provide the basis for nationally consistent regulation of privacy and the handling of personal information;

(e) promote the responsible and transparent handling of personal information by agencies and organisations;

(f) facilitate the growth and development of electronic transactions, nationally and internationally, while ensuring respect for the right to privacy;

(g) establish the Australian Privacy Commission and the position of the Privacy Commissioner; and

(h) provide an avenue for individuals to seek redress when there has been an alleged interference with their privacy (APLP, p26-27).

1.1. Preservation notices and privacy issues

The *Telecommunications (Interception and Access) Act* was amended by the *Cybercrime Legislation Amendment Act 2012* (Cth), which was passed by both houses of parliament on 22 August 2012 and came into effect on 10 October 2012. A substantial aspect of the amendment related to "preservation notices". Under the new ss 107H to 107W, a preservation notice can require the carrier to preserve all stored communications that the carrier holds relating to the person or communications service specified in the notice. This section also applies when the stored communication is requested from the Australian Federal Police on behalf of certain foreign countries.

This Act has been criticized as there are no restrictions on the use of information requested by foreign countries. Senator Scott Ludlam (commenting on the amendment) also said in the Senate that it was deeply concerning that countries with less strict privacy legislation than Australia could request personal information on Australians under investigation, and such requests cannot be refused. He stated, "Given the medium that we now operate in, privacy protections can be absolutely rock-solid in Australia, but if we are sharing data—intimate personal details of people's lives—with law enforcement and intelligence agencies in foreign jurisdictions with lower standards of privacy protection that we have in Australia, and that material leaks, then the privacy protections that they're afforded in Australia [are] worthless, because that information can be back in Australia at the speed of light."

Recommendations

EFA recommends restrictions on the use of information requested by foreign countries. The Act should protect the privacy of Australians by ensuring that there is a right to refuse requests for data or personal information from foreign countries in certain exceptional circumstances (Recommendation 1.1.1 c) Changes to Part 3 Section 107R inclusion of d) and e).

a) Changes to Part 3 section 107N:

Changes to Part 3 section 107N: (2) In the notice, the Australian Federal Police can only specify:

(a) one person; or

(b) one or more telecommunications services; or

(c) one person and one or more telecommunications services.

107N 2(c) "one person and one or more telecommunications services" should be removed, requiring multiple foreign preservation notices if "one person and one or more telecommunications services" require preservation, as the privacy and protection of individuals **not** under investigation could inadvertently have their information and records provided to foreign law enforcement agencies.

b) Changes to Part 3 section 107P:

Changes to part 3 section 107P: (2) The request to the Australian Federal Police must:

(a) be in writing; and

(b) specify the name of the authority concerned with the criminal matter; and

(c) specify the serious foreign contravention that is the subject of the investigation or investigative proceeding; and

(d) specify information identifying the stored communications to be preserved and the relationship between those communications and the serious foreign contravention; and

(e) specify any information the foreign country has that identifies the carrier that holds the stored communications; and

(f) if the stored communications relate to a specified person—specify any information the foreign country has that identifies the telecommunications service to which the stored communications relate; and

(g) specify the reasons why the stored communications need to be preserved; and

(h) specify that the foreign country intends to make a request under paragraph 15B(d) of the Mutual Assistance in Criminal Matters Act 1987 to access the stored communications.

107P 2 (d), (e) and (f) permit requests to have unnecessarily wide scope, including material that is unrelated to the foreign contravention investigations. Such "fishing expeditions" result in unnecessary intrusions into the privacy of individuals. Therefore an additional clause (i) is required that includes the wording "private or identifiable information of individuals data that is collected under the foreign preservation notice, but not identified in that notice, be removed from the preserved data before the stored data be submitted to the foreign agency. This includes all information of a private nature unrelated in any form to the foreign contravention that the foreign preservation notice stored communications period covers."

c) Changes to Part 3 section 107R:

Changes to part 3 section 107R: inclusion of a section (4) that allows the revoking of a foreign preservations notice where multiple notices are received and can currently be received under 107N 2(c). For example the following should be included:

(a) where, as a result of previous foreign preservation notices the use of additional foreign preservation notices can be considered as a fishing expedition, and/or

(b) where an individual is identified that was previously unidentified, but has now been included as a result of private information being obtained that would not have been obtained had the recommendations in 107P been in place, and/or

(c) where there are no strict stipulations of the use of stored communications outside the specific contravention outlined in the foreign preservation notice, and/or

(d) when the foreign countries have not been able to provide justification for their requests, and or

(e) when they have no method of ensuring that the private information of Australians are adequately protected and kept in a secure manner when they receive the information.

1.2. Better protection of privacy is required

The *TIA Act* provides two sets of processes for accessing information depending on whether it is content or metadata. Although the PJCIS Inquiry recommends considering "proportionality tests" for all interceptions the situation is most dire for metadata, which they call "telecommunications data".

Within Part 4 the only consideration for privacy is s 180F: "Before making an authorisation under Division 4 or 4A in relation to the disclosure or use of information or documents, the authorised officer considering making the authorisation must have regard to whether any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable, having regard to the following matters:

(a) the likely relevance and usefulness of the information or documents;

(b) the reason why the disclosure or use concerned is proposed to be authorised".

Recommendations

a) Changes to Part 4B section 180F

Changes to Part 4B section 180F preamble to include "information, documents, images, audio recordings, whether they be digital or otherwise constructed and stored", which should then read:

> "*Before making an authorisation under Division 4 or 4A in relation to the disclosure or use of* information, documents, images, audio recordings whether they be digital or otherwise constructed and stored*, the authorised officer considering making the authorisation must have regard to whether any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable, having regard to the following matters:*

b) Changes to Part 4b section 180F (a)

Changes to Part 4b section 180F (a): inclusion of "information, documents, images, audio recordings whether they be digital or otherwise constructed and stored" Section (a) to read:

> (a) the likely relevance and usefulness of the information, documents, images, audio recordings whether they be digital or otherwise constructed and stored;

1.3. Improving protections for metadata

It is submitted that message content and "metadata" (referred to as "telecommunications data" within the *TIA Act*) should no longer be treated separately. Currently access to these is regulated by Part 2 and Part 4 of the *TIA Act* respectively. Metadata can be accessed much more easily than message content as it does not require a warrant and the privacy considerations are relatively weak.

There is no reason to maintain this distinction in future revisions of the *TIA Act*. The significance of metadata and the privacy implications of revealing it are well known; its interception and access should not be subject to lesser scrutiny and oversight.

The internet is not like a fixed line telephone.

> *"5.66 Mr Bernard Keane, submitting in a private capacity, argued that extending data retention from fixed line and mobile telephones to the internet constitutes a significant expansion of the powers held by law enforcement and security agencies, and thus would constitute a significant intrusion on privacy:*

"Australians, like citizens around the world, do not use online communications in the same way, or for the same purposes, as they used phones. They did not commit huge amounts of personal information to permanent storage on the phone. They did not leave crucial financial details on the phone. The phone was not their primary tool for interacting with communities that are important to them. The telephone did not enable contact with communities around the globe that are of critical importance to citizens."

> *5.67 As such, Mr Keane posited that:*

Any attempt therefore to impose the telecommunications interception laws on the internet represents not a logical extension of that law to 'keep up with technology' on a like-for-like basis but a dramatic extension of surveillance into citizens' lives far beyond that enabled by telecommunications interception.

> *5.68 Mr Ian Quick, submitting in a private capacity, expressed a similar concern to that of Mr Keane, noting that if data on internet browsing is retained, this would constitute a much greater invasion of privacy than telecommunications data:*
>
> *It is a massive invasion of everyone's privacy, as the usage database will contain every page they accessed – such as every article they have read on a newspaper site, any online political activity they have done, anything they have done on ebay, what books they have bought on Amazon, ..."*

In many digital communications, the distinction between metadata and content is significantly eroded. For example, when using a web based service the URLs of web requests would constitute metadata. A list of URLs accessed would effectively constitute a detailed account of user interaction. Rather than telling us that the user visited a library, metadata would provide a list of which pages of individual books were read. This potentially detailed information should require more oversight than metadata of phone and mail services that provides only "envelope" information. In addition, significant personal information may sometimes be encoded in URLs. For example this might include account information of financial or other personal services and other very specific private information that accompanies 'content' information.

The appraisal of privacy in these situations has already been entertained by Sotomayor in her 2012 concurring judgement in US v Jones: "I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled" to privacy protection.

Further, the value of metadata *over* content is actually a known best practice in commercial ventures: Facebook's market value is not borne from the content of user posts, or even that they continue to log in. User patterns of "liking" and sharing and their associations with other users create enormous value that is not derived directly from message content. These associations jump across demographic, geographic and other borders to provide new insights that can erode privacy. These associations are used to create specifically vectored advertising. Further, retaining such data can create a "honey pot" that is itself a security threat.

The classic political-personal intrusion of these practices was exemplified in an empirical study of 4,080 Facebook profiles that determined the sexual orientation of individual users whether or not they disclosed that information on their own by analysing the friendship lists of self-identified gay men (Jernigan et al. 2009). The content of our posts become irrelevant; our metadata defines us.

Likewise, Google has become less interested in the content of our searches and instead hopes the omnipresent data retention of Google+ will allow deeper insight into people's digital lives:

> *"The value of Plus has only increased in the last year, as search advertising, Google's main source of profits, has slowed. At the same time, advertising based on the kind of information gleaned from what people talk about, do and share online, rather than simply what they search for, has become more important."*

As per the Victorian Privacy Commissioner, data retention is 'characteristic of a police state' as it goes against both the presumption of innocence, and 'essential dimensions of human rights and privacy law: freedom from surveillance and arbitrary intrusions into a person's life'

Consistent treatment of message content and metadata is also supported by the Law Council of Australia:

> "… the Law Council supports the inclusion of a single, consistent privacy test in all warrant applications and in all authorisations to intercept, access or disclose telecommunications or telecommunications data."

Recommendations

EFA is concerned that digital data and communications from telecommunications networks are being included in domestic and foreign preservation notices. EFA suggests that one of two approaches is taken: either the *TIA Act* is amended so that privacy-intrusive metadata cannot be supplied, or the metadata regulations are merged with those concerning message content so that their protection can be enhanced.

Option a) Limiting the Act's scope to preclude metadata

Changes to Part 1-2 Section 5A, include the following definition:

> (a) The telecommunications (Interception and Access) Act 1979 is limited to audio recordings and limited meta data related to telephone use that does not include:
>
> (i) software, and
>
> (ii) data streams, and
>
> (iii) digital images, and
>
> (iv) digital audio or sound files that are not attributed directly to a telephone call, and
>
> (v) any other transmitted digital traffic that uses an internet browser or internet connection for transmission.

Option b) Eliminate differences between content and metadata protection

Data intercepted in all its forms be referred to as "data intercepted". Parts 2 and 4 of the *TIA Act* shall be merged to allow more stringent controls and oversight of access to non-message content data, similar to those governing content.

1.4. Privacy of digital objects

Details of the 'For Your Information: Australian Privacy Law and Practice' recommendations (p257-292) provided in the May 2008 report is limited in addressing digital data as an object (hereafter referred to as digital object) that needs protecting under the Privacy Act. This digital object, containing human information that would be considered of a private nature (see OAIC), especially where an organisation has a business or professional relationship with the individual is of particular concern. While IPP 1-3 identifies the privacy of an individual's information, which includes all Digital Objects (documents, databases, audio recordings or pictures), additional digital objects including IP Addresses, digital, virtual, mobile or landline data that could lead to the identification of telephone numbers and associated addresses of individuals linked either directly or indirectly to those digital objects should be identified and addressed specifically within the Telecommunications (Interception and Access) Act 1979.

Recommendations

Additional digital objects such as IP addresses, digital, virtual, mobile or landline data should be identified and addressed specifically within the Telecommunications (Interception and Access) Act 1979.

1.5. Use of intercepted material as evidence in criminal proceedings

The TIA Act allows intercepted information to be adduced as evidence in criminal proceedings. In contrast, in the United Kingdom, the Regulation of Investigatory Powers Act 2000 (RIPA), does not generally allow intercepted information to be used as legal evidence in criminal proceedings. The RIPA governs the interception of communications in the United Kingdom and so is a 'sister Act' to the TIA Act. It grants extremely wide-ranging powers and permits an extensive number of 'Relevant Public Authorities' to intercept private communications.

The rationale behind this is so that the intercepted material can be used to detect and prevent terrorism and serious crime. As stated by the House of Lords in R v Preston:

> *"Those who perform the interceptions wish to minimise the dissemination of the fact that they have been performed, since it is believed that this would diminish the value of activities which are by their nature clandestine. We need not consider to what extent this preoccupation with secrecy at all costs is soundly based for it has been treated as axiomatic for decades, if not longer."*

Sections 18 (7) and 18 (8) of RIPA states:

> 18 (7) Nothing in section 17(1) shall prohibit any such disclosure of any information that continues to be available for disclosure as is confined to—
>
> (a) a disclosure to a person conducting a criminal prosecution for the purpose only of enabling that person to determine what is required of him by his duty to secure the fairness of the prosecution;
>
> (b) a disclosure to a relevant judge in a case in which that judge has ordered the disclosure to be made to him alone; or
>
> (c) a disclosure to the panel of an inquiry held under the Inquiries Act 2005 or to a person appointed as counsel to such an inquiry where, in the course of the inquiry, the panel has ordered the disclosure to be made to the panel alone or (as the case may be) to the panel and the person appointed as counsel to the inquiry; or
>
> 18 (8) A relevant judge shall not order a disclosure under subsection (7)(b) except where he is satisfied that the exceptional circumstances of the case make the disclosure essential in the interests of justice.

Section 18(9) states that the judge may, if after considering the disclosed intercepted material, believe that exceptional circumstances exist, may direct the prosecution to make an admission of fact regarding the intercepted material. However, s 17(l) prevents the prosecution from divulging the fact of interception.

Recommendation

The TIA Act should not allow intercepted information to be adduced as evidence in criminal proceedings, except in exceptional circumstances (similar to the United Kingdom's RIPA).

2. Australia's National Security Legislation report, dated May 2013

2.1. Who can access data

In addition to maintaining a high threshold for access to telecommunications data, it is critical that the number of agencies that can access this data is kept to the bare minimum. This was a particular problem for RIPA in the UK, which is a lesson that Australia can learn from.

In 2008, a series of scandals highlighted the serious potential for misuse of power when it was discovered in UK in June 2008 that 121 councils had used the legislation during a 12-month period to monitor behaviour by examining the private communications of residents in order to determine whether residents were lying about living in particular school catchment areas. (see, for example, Poole council loses school catchment 'spying' tribunal, BBC, 2 August 2010,

http://www.bbc.co.uk/news/uk-england-dorset-10839104).

In Australia, Telecommunications data is restricted to 'enforcement agencies', as defined in s 5 of the Act. The bodies listed in this section include a number of law enforcement agencies, as well as the following:

"(n) any body whose functions include:

i. administering a law imposing a pecuniary penalty; or

ii. administering a law relating to the protection of the public revenue."

Chapter 3 of the *Attorney General's Telecommunications (Interception and Access) Act 1979 Annual Report 2012-13 provides information on 'enforcement agencies' that had gained authorisations to access telecommunications data in accordance with ss 186(1)(b) and 179 of the Act. These included bodies that were not affiliated with law enforcement in any capacity – including a number of councils, state racing bodies and state branches of the RSPCA, and Australia Post.*

Furthermore, a total of 5 authorisations were made to foreign law enforcement agencies. However, the report was silent on who the bodies were.

Fewer agencies means less chance of misuse and, realistically, if the threshold for access is kept to 'serious crimes' then this instantly limits the agencies that might need access.

Recommendation

The number of agencies that can access one's personal data should be kept to the bare minimum. Particular attention should be given to the definition of 'enforcement agency' in s 5 of the Act mentioned above, and all relative provisions thereafter.

2.2. Attorney-General's guidelines

The Attorney-General's Guidelines directing ASIO's collection of data about Australians requires them to minimise the amount of data collected in order to carry out their functions. It also spells out fairly detailed requirements for running "Investigations". Unfortunately there are a few key caveats:

- The public has no way to know how many investigations into subjects there are, or how many people are subjects of investigations

- *4.1(c) "subject" means a person, group or other entity* (this could, for example, be interpreted to include everybody in Tasmania)
- *10.1 Information obtained by ASIO is "relevant to security" where it may assist in determining whether:*

  (a) there is a connection or possible connection between a subject and activities relevant to security, irrespective of when such activities have occurred or may occur;

  (b) the activities of a subject are not relevant to security

This would mean that one could be placed under surveillance and it would be relevant to security because they're trying to find out if what one is doing is relevant to security. Such caveats would allow for fishing expeditions.

Recommendation

The AG's Guidelines should be revised so that the above mentioned caveats do not give ASIO such wide powers to collect data. It is suggested that ASIO's privacy guidelines should be an extension of the guidelines used for accessing ordinary telecommunications data, scaled up to cover the cases of heightened seriousness and more severe privacy intrusions for which ASIO is authorised.

2.3. ASIO is not included in TIA Act reporting

Section 186 of the *TIA Act* concerns requirements to report to the minister the number of authorisations made under Part 4. It states that "*an enforcement agency must give the Minister…*" where *enforcement agency* is a list of agencies that notably does not include ASIO, the one intelligence agency in Australia that has the right to collect intelligence from Australians. In the interests of transparency, similar metrics should be recorded and publicly reported for ASIO. It will inevitably be argued that even this modest requirement would pose an unreasonable threat to national security. The onus must be placed on the law enforcement community to explain with clear examples how this kind of report could aid or abet enemies of the state.

Recommendation

ASIO should be included in TIA Act reporting. In the interests of transparency, similar metrics should be recorded and publicly reported for ASIO.

3. Conclusion

EFA believes that the *TIA Act* as it stands does not adequately protect the privacy and civil liberties of Australians. It also does not assist in promoting national security as effectively as it could. Data retention is an ineffective method to curb terrorism.

Those acting against national security will not be affected by data retention. The ease with which data retention regimes can be evaded is grossly disproportionate to the cost and security concerns of the data retention regime. Without public evidence to the contrary, the electorate can only proceed with the facts before them. Data retention regimes provide security and privacy risks for citizens, while are easily mitigated by criminals and terrorists.

The law needs to be reformed so that citizens' rights, especially the right to privacy, are better protected. The *TIA Act* should place tighter regulations on who can access data. Further, the legislation should be updated in light of technological advancements. EFA believes that these amendments would provide a better balance between the interests of national security and protecting individual privacy.