



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
T @efa_oz

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House, Canberra ACT 2600

Via email to: pjcis@aph.gov.au

6th August 2014

Dear Committee Secretary,

Re: Inquiry into the National Security Legislation Amendment Bill (No. 1) 2014

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

Celebrating its 20th anniversary in 2014, 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 digital 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 digital communications systems.

Yours sincerely,

Jon Lawrence
Executive Officer



Submission to the Inquiry into the National Security Legislation Amendment Bill (No. 1) 2014

Introduction

EFA understands the challenges that Australia's intelligence and law enforcement agencies face in the context of rapid technological change where communications are becoming increasingly digitised.

EFA supports the appropriate, proportionate and reasonable reform of legislation to ensure that Australia's intelligence and law enforcement agencies are equipped to detect, investigate and prosecute serious criminal activity that threatens the peace and security that Australians have long enjoyed.

Turbulent times have seen new and advanced threats to Australia's national security, including home-grown terrorism, Australian extremism abroad and the constant and real risk of cyber-espionage from state and non-state enemies. EFA agrees with many of the Recommendations in Chapter 4 of the PJCIS Report, and can understand the need for greater integration between national security bodies and the private sector.

EFA does, however, hold a number of caveats to the overall benefit to the Australian public, especially when national security is weighed up against civil liberties. While many of the proposed reforms are justifiable on face value, many others are not, and EFA asserts that they pose a significant threat to the balance between national security and online privacy and liberty.

EFA is seriously concerned with the extension of ASIO's powers in a number of areas, most notably in their authorised access to third parties or computers in order to carry out an investigation. EFA asserts that such powers are wholly disproportionate with the threat they pose to the privacy of innocent parties. EFA fears that this intrusion may result in significant privacy 'collateral damage'.

Certain Recommendations, which will be discussed further below, also give ASIO the power to potentially act far outside the scope of the original intention of the power.

Mandatory Data Retention

EFA understands that the issue of mandatory data retention is expressly excluded from this submission. EFA would like to make it clear that the decision to do so, particularly in light of recent media reports suggesting the government has decided to move quickly to implement such a scheme, undermines the contextual effectiveness of the following discussion.

EFA is firmly opposed to any data retention initiative. Please refer to our previous submission to the PJCIS.¹

¹ Available online at

http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/ns12012/subs/sub121.pdf

Proportionality

The PJCIS's recommendations repeatedly emphasise that interception or privacy intrusions should be "proportionate" to the national security threat, offence or other matter that is under investigation, particularly within the context of the *Telecommunications (Interception and Access) Act 1979*.

EFA contends that the same concept should be applied to any new powers to be granted to ASIO, whose activities in this case constitute an advanced form of interception.

EFA is a signatory of the *International Principles on the Application of Human Rights to Communications Surveillance*², and believes that these principles should be closely considered by the Committee in reviewing this proposed legislation.

In particular, EFA wishes to draw the Committee's attention to the section on *proportionality*:

Communications surveillance should be regarded as a highly intrusive act that interferes with human rights threatening the foundations of a democratic society. Decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests.

This requires a State, at a minimum, to establish the following to a Competent Judicial Authority, prior to conducting Communications Surveillance for the purposes of enforcing law, protecting national security, or gathering intelligence:

- 1. there is a high degree of probability that a serious crime or specific threat to a Legitimate Aim has been or will be carried out, and;*
- 2. there is a high degree of probability that evidence of relevant and material to such a serious crime or specific threat to a Legitimate Aim would be obtained by accessing the Protected Information sought, and;*
- 3. other less invasive techniques have been exhausted or would be futile, such that the techniques used is the least invasive option, and;*
- 4. information accessed will be confined to that which is relevant and material to the serious crime or specific threat to a Legitimate Aim alleged; and*
- 5. any excess information collected will not be retained, but instead will be promptly destroyed or returned; and*
- 6. information is will be accessed only by the specified authority and used only for the purpose and duration for which authorisation was given.*
- 7. that the surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or of fundamental freedoms.*

² Available online at <https://en.necessaryandproportionate.org/text>

Definitions

EFA asserts that the amended definition of ‘computer’ in sections 4 and 22 of the *ASIO Act* is too expansive and may provide a single warrant holder with an enormous number of possible computers to target.

EFA notes that by amending the definition of ‘computer’, and expanding it substantially to include multiple devices, systems or networks, this single amendment would expand the scope of ASIO’s powers in a number of other places within the *ASIO Act*.

This minor amendment, relative to the entirety of the act, would have a wildly disproportionate effect on the scope of every single warrant involving a ‘computer’. EFA cannot condone such a rash escalation of warranted power and recommends that a more carefully defined definition be provided.

Disruption

Recommendation 21 invited the Government to consider enabling ASIO to disrupt a target computer for the purpose of executing a computer access warrant. The PJCIS report tabled in June 2013 included a qualification that the Government should “pay particular regard to the concerns raised by the Inspector-General of Intelligence and Security”.

These concerns related to the impact of the disruption upon unrelated users and stated that there is a “need to balance the potential consequences of this interference to the individual(s) with the threat to security”. No such balancing is included in the Bill.

Section 25A(5) is replaced with:

(5) Subsection (4) does not authorise the addition, deletion or alteration of data, or the doing any thing, that is likely to:

- (a) materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer unless the addition, deletion or alteration, or the doing of the thing, is necessary to do one or more of the things in the warrant; or
- (b) cause any other material loss or damage to other persons lawfully using a computer.

In other words, once a warrant is granted there are no protections at all unless there is “material loss or damage”. EFA asserts that such a high standard of contravention of this section would, by default, allow all other passage into innocent parties’ devices. EFA can confidently assume ASIO’s capacity to compromise a computer(s) without detection, and as such, this proposed amendment would give ASIO ‘safe passage’ for potentially unlimited routes to achieving the warrant’s purpose.

There are various problems that arise. These include:

- Timestamps or file contents could be affected that would alter the outcome of a prosecution of the target;

- Modifying network traffic could result in log files being generated on third party computer systems that misrepresent the activities of the target;
- This section may permit serious “disruptions” that go beyond what is necessary to execute the warrant (for example, installing secret bugs on a computer); and
- ASIO’s techniques may be suppressed on national security grounds, making it difficult to assess the quality of evidence relating to any computer or network traffic.

The proposed wording of this amendment is of particular concern. Australians are not protected by any constitutional right to privacy, nor any legal expectation of privacy. Accordingly, Australians are in a vulnerable position when arguing that a breach of their privacy *per se* is material loss. Furthermore, when coupled with the expanded definition of ‘computer’ mentioned above, it would allow ASIO to effectively access, intercept, disrupt, delete, alter or otherwise ‘materially interfere with’ multiple computers or computer *networks* with a single warrant.

EFA recommends that this provision be removed, as it disproportionately extends the scope of ASIO’s warranted powers.

Access via third-party computers

Recommendation 22 was that the Government should allow ASIO to access third party computers and communications under a computer access warrant. This was on the condition that it was “subject to appropriate safeguards and accountability mechanisms”. No such safeguards and accountability mechanisms are included in the Bill.

The previous PJCIS was correct to characterise this as “hacking” the computers of people who are not threats to security. Although the Attorney-General’s Department seeks to draw a distinction between hacking merely to obtain access to another computer, and use of that hack to examine the content of the innocent computer, many problems are created simply by the act of breaking into that computer.

All businesses have legal obligations and commercial interest in maintaining the security of their computer systems. If an external intrusion is detected, it is best practice IT management to reset passwords and rebuild all affected systems from scratch using software from trusted sources.³ If ASIO broke into a third party computer without their cooperation, this could cause an enormous amount of damage to that business and inconvenience to their users.

For ASIO to be able to take this kind of action against a third party who maintains their computers well they will need to stockpile exploits for 0-day vulnerabilities.⁴ This means that we will have a Government agency actively seeking and hoarding methods of breaking into innocent Australian computers instead of helping them to secure themselves. These vulnerabilities may also be known

³ This Cisco whitepaper demonstrates the extent of work that should ordinarily be undertaken when a security breach is detected:
http://www.cisco.com/warp/public/cc/so/neso/sqso/roi3_wp.htm

⁴ 0-day vulnerabilities are security flaws in computer software that are not publicly known and have not yet been fixed by the software vendor. These are valuable and frequently traded on black markets.

by foreign states or criminals, which means that there is a heightened risk of other hacking crime being perpetrated against Australians.

Various situations need to be contemplated to ensure that the law offers appropriate protections:

- Would a third party be subject to any penalty for publicising information about being attacked by ASIO, including the attacker's identity or the activities that were performed using their computer?
- If a third party realised that they were attacked by law enforcement, would any penalty be attracted for actively warning their users of the system compromise, as would normally be good practice?
- If ASIO caused damage to the third party's computer or reputation in the course of executing the warrant would the third party have any opportunity to claim damages?

EFA believes that there are too many problems with this amendment without further regulations on the circumstances in which this capability can be used. If use of a third party computer is absolutely required to execute a warrant it would be far preferable to coerce the third party to assist in the investigation, with appropriate oversight and appeal processes.⁵

Cooperative Intelligence Operations

Recommendation 39 appears to have been implemented in Schedule 5 of the *Intelligence Services Act 2001*. Section 13B permits ASIS to assist ASIO with overseas parts of their investigations targeting Australians. The only limitation on the scope of these activities is Section 13D, which limits ASIS to what ASIO could do in Australia if it were authorised by warrant.

It is highly inappropriate that ASIS should be authorised to perform acts without a warrant that would require a warrant for ASIO to perform them in Australia. This is particularly sensitive when many Australians' data and communications traverse or are stored in foreign countries.

This is quite different from IGIS's suggestion put forward by the previous PJCIS that a common standard be developed for intrusive activities involving the collection of intelligence about Australian persons.

EFA opposes a reduction in the rights of Australians simply because ASIS is performing them overseas. The idea suggested by IGIS, however, has merit, but it does not appear to have been used by the Government in this case.

Penalties for disclosure of classified information

The proposed new Section 35P of the *ASIO Act* does not clearly follow any PJCIS recommendation. It provides 5 and 10 year imprisonment penalties for a person who discloses information about a special intelligence operation.

This new section is non-specific about the type of person disclosing the information; it would therefore cover both employees of ASIO and journalists. There is no provision for whistleblowing –

⁵ The United States offers a good example of inappropriate appeal processes. Their *National Security Letters* coerce cooperation and gag the target from revealing its existence. Their only redress is via the secret Foreign Intelligence Surveillance Court.

and so no protection for disclosure of classified information where it is in the public interest to do so.

EFA can understand the need for confidentiality of intelligence operations. However, EFA is deeply concerned with the proposed reforms as they stand for the following reasons:

1. 'Special intelligence operation' is defined in section 4 of the Act, but is defined broadly and is open to a wide scope of interpretation; and
2. There is no way for a journalist with leaked material to know what is and is not part of a 'special intelligence operation'.

We note that the proposed drafting of section 35P does not make any concession for a fault element, and instead the offence appears to carry absolute liability. EFA fears that such strong wording, and very limited exceptions, may leave parties vulnerable to severe punishments if they report on, what they had no knowledge was, a special intelligence operation. The proposed section 35P, as it stands, has perilous implications for any journalist who does not intend on compromising public safety, but inadvertently does so.

The actions of Edward Snowden have shown that there is great value in responsible whistleblowing. His leaks have demonstrated that the US National Security Agency has been engaged in illegal activities. His disclosure and publishing by various news outlets including *The Guardian*, *New York Times* and *Washington Post* have directly prompted reforms. Section 35P of the Bill may have the effect of criminalising this type of journalism if evidence of similar wrongdoing occurred in Australian agencies.

Famed NSA whistleblower Thomas Drake summed up the risks well with his comments on this Bill:

*"If this passes in its current form without huge changes, it is going to send a very chilling message," Mr Drake said. "It will create a climate in which people will self-censor. They will opt not to reveal anything. They will opt not to associate with certain individuals. They will opt not to share certain information just on the risk that it might be designated secret or it might be designated something that might reveal an intelligence operation. Well in that kind of an environment guess what? It has its intended effect."*⁶

Andrew Wilkie, MP for Denison, a former member of PJCS, released a statement suggesting that additional amendments are required to enable disclosure in the public interest:

*"The increase in penalties for the disclosure of intelligence material must also be accompanied by an amendment to the Public Interest Disclosure Act 2013 to ensure protection for intelligence whistle-blowers. Currently intelligence material and intelligence officials are not covered by this legislation."*⁷

⁶ Ben Grubb, "Edward Snowden's lawyer blasts Australian law that would jail journalists reporting on spy leaks", Sydney Morning Herald, 30 July 2014. Available online at <http://www.smh.com.au/digital-life/consumer-security/edward-snowdens-lawyer-blasts-australian-law-that-would-jail-journalists-reporting-on-spy-leaks-20140730-zyn95.html>

⁷ This statement is available on Andrew Wilkie's website: http://www.andrewwilkie.org/content/index.php/awmp/press_extended/a_statement_on_the_governments_proposed_security_changes



The purpose of this Recommendation is clear - to dissuade any dissemination of confidential information into the public domain. The risks of same are also well-established - such a leak may affect Australia's national security; it may compromise our diplomatic affairs and it may potentially reveal strategic and operational strategies. EFA does not contest any of the above rationales.

EFA is, however, concerned that no proportionate provisions are being proposed to allow for the dissemination or 'leaking' of information that is *in the public interest*. Ultimately, if flaws, corruption or abuse of power are in fact present within Australia's law enforcement and intelligence agencies, the exposure of same should be protected in circumstances aforementioned.

EFA recommends that in order to protect the integrity of freedom of speech, open media and public interest, the PJCIS consider the following aspects of the proposed section 35P as it stands:

1. The broad interpretation of 'special intelligence operation';
2. A broader list of exceptions;
3. A clear and reasonable fault element, preferably requiring intention or recklessness on behalf of the reporter;
4. In the alternative to (3) above, the inclusion of defences (not just exceptions); and
5. The inclusion of a 'public interest' defence, or alternatively, proportionate whistleblower protections in other legislation.

Review period for new legislation

EFA believes that this review period is too short for many stakeholders to submit in detail and makes it difficult for the PJCIS to review such a large and complex bill in as much detail as is required.

If the PJCIS determines that this quality of this inquiry has been compromised by the short timeframe, EFA would suggest that this should be stated in the report so that appropriate scrutiny can be encouraged in the future.