Electronic Frontiers
AUSTRALIA

PO Box 1302, Kensington VIC 3031
T +61 3 9013 9492 F +61 3 9013 9468
E email@efa.org.au W www.efa.org.au
ABN 35 050 159 188

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

20th August 2012

Dear Secretary,

Thank you for providing the opportunity to make a submission to the Committee's inquiry in relation to the Attorney-General's discussion paper on proposed legislative expansion of national security powers.

Electronic Frontiers Australia Inc. (EFA) is a non-profit national organisation representing Internet users concerned with on-line rights and freedoms. EFA was established in January 1994 and incorporated under the Associations Incorporation Act (S.A.) in May 1994. The website address is www.efa.org.au.

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.

EFA policy formulation, decision making and oversight of organisational activities are the responsibility of the EFA Board of Management. The elected Board Members act in a voluntary capacity; they are not remunerated for time spent on EFA activities.

EFA has presented written and oral testimony to State and Federal Parliamentary Committee and government agency inquiries into regulation of the Internet and online issues.

Please find following the issues of particular concern that we have highlighted in our review of the Terms of Reference and associated Discussion Paper. EFA would be pleased to expand on the issues below in oral testimony or otherwise.

Yours faithfully,

David Cake, Chairperson,
On behalf of the Board, Electronic Frontiers Australia Inc

General opening statements

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 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 that threatens the peace and security that Australians have long enjoyed.

EFA is however concerned that despite the Discussion Paper displaying a relatively sophisticated understanding of the 21st century telecommunications ecology, and despite mentions of Australians' right to privacy, the Paper is written from an essentially authoritarian perspective.

There have been massive increases in surveillance powers granted since 2001 that have significantly altered the balance between the freedoms that these powers are ostensibly designed to protect, and the potential harm to those freedoms that these powers can represent.

Privacy and freedom of expression are fundamental human rights, and are necessary for the continued functioning of a free and democratic society. Any constraints that are to be placed on an individual's privacy or their freedom to express themselves must therefore be limited to those where it can be clearly demonstrated that the constraint is necessary to benefit the society as a whole.

The proposals contained in the Discussion Paper, if implemented in full, would amount to an unprecedented programme of mass surveillance that would invade the privacy of all Australians in the name of catching a tiny minority of serious wrong-doers.

If citizens are required to agree to expanded conditions of surveillance, they also deserve commensurate positive protections. These include both general protections—reasonable expectation of privacy when using telecommunications systems, no collateral surveillance—and serious protection and accountability if privacy is breached, whether the breach is by government employees or third parties.

Indeed, even leaving aside the 'honeypot' issues of data retention, recent Government and contractor failures in this regard (such as the AusCERT subscriber DVD postage loss) demonstrate that significant headway must be made for Australians to trust that extended surveillance, even in the national interest, has their interests at heart.

In addition, EFA is seriously concerned with the manner in which these proposals have been produced. The period of time allowed for public input (originally a mere four weeks, later extended to six weeks) is entirely inadequate for such a broad range of proposals, even if they were well-defined and clearly articulated. The reality however is that the Terms of Reference and associated Discussion Paper are far from coherent, including a number of proposals that are mentioned without any attempt at a comprehensive definition, let alone any meaningful attempt at justification.

The most glaring example of this is the data retention proposal, which merits a single sentence in the Terms of Reference and is effectively completely absent from the Discussion Paper. This proposal is arguably the most egregious of the proposed new powers that the Committee has been

asked to consider, and it is therefore difficult not to conclude that the absence of any detail in relation to this proposal represents a deliberate attempt on the part of the Attorney-General's Department to reduce the degree of public scrutiny to which this proposal would otherwise be subjected.

EFA is aware that the Attorney-General's Department has undertaken consultations in relation to this proposal with the telecommunications industry, but believes that this is wholly inadequate as these consultations have not included community organisations, such as the Australian Privacy Foundation, the Internet Society of Australia, EFA itself, and other civil liberties organisations.

EFA is further concerned that a number of these proposals continue the process of co-opting the private sector into the national security apparatus. EFA is fully aware that the Internet is a global communications network that is largely operated by the private sector, so it is inevitable that the private sector must have some role in the process of surveillance, however there need to be clear limits on the extent to which the costs of surveillance are out-sourced. The dangers of out-sourcing the costs of surveillance to the private sector are that it removes the accountability that would apply were these costs met from government revenue, and that it creates incentives for commercial entities to undertake actions to recoup their costs in relation to surveillance, that are likely to further erode the privacy and civil liberties of their customers.

Electronic Frontiers AUSTRALIA

Data retention

Relevant Act: *Telecommunications (Interception and Access) Act 1979*

Terms of Reference extract:

15. Modernising the Industry assistance framework

a. tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities, and privacy and cost impacts

Submission

Detail of the proposal

EFA is seriously concerned at the lack of detail provided by the Attorney-General's Department in relation to this proposal, as well as the lack of any cost-benefit analysis or even a substantive justification for such a wide-ranging proposal that would affect all Australians. It is therefore very difficult to make meaningful comments on a proposal that lacks any substantive detail.

EFA recommends that the Committee reject this proposal out of hand, and request that the Attorney-General's Department provide a detailed proposal that includes an explanation of the justifications behind it and a cost-benefit analysis.

Benefits to law enforcement and intelligence agencies

The ostensible justification for a mandatory data retention scheme is to benefit police investigating criminal activity both online and offline. EFA feels that far from being obvious, the benefits for crime fighting are highly questionable. To justify the advent of what amounts to widespread surveillance of the Australian public, a detailed case must be made that current sources of information are inadequate for the prosecution of certain crimes. EFA does not believe that crime "prevention" can be used to justify a system that would collect data on the entire population, regardless of whether they are suspected of a crime or not.

It is worth noting that determined criminals will have little difficulty disguising or anonymising their communications. There are many relatively simple and very effective tools available that allow for the protection of communications from surveillance. While these tools will not be appealing to the vast majority of users as they can degrade connection speeds and reduce functionality, they are a viable option for those individuals that are determined to communicate in secrecy.

It is therefore highly questionable whether a new and broad data retention scheme would aid in the investigation of terrorism, organised crime, or other serious illegal activities.

EFA feels that any move to introduce data retention laws that could negatively impact the privacy of Australian citizens should begin with a detailed accounting of how this scheme will bring tangible benefits to the community through a reduction in crime. Clearly, a law of diminishing returns applies as the volume of data recorded about the public's communications increases. There is a genuine danger that the creation of massive oceans of data could in fact impede, rather than improve, the ability of law enforcement to utilise such data as part of their investigations; a case of too much, rather than too little data.

Transparency

EFA feels very strongly that any proposal for a data retention scheme must be dealt with as transparently as possible. Firstly, with regard to the implementation of the scheme, EFA feels that the Australian public should be consulted from the beginning.

Secondly, in operation the scheme must be as transparent as possible as well, so that members of the public are able to be fully aware of which aspects of their communications may be recorded. EFA does not accept that such transparency would somehow aid criminals or put Australians at risk.

Privacy issues

EFA's primary concern with a mandatory data retention requirement is the unprecedented threat that it would represent to the right to privacy of all Australians. Our communications with business, colleagues, friends and loved ones are among the most sensitive information any of us will generate in our daily lives.

A blanket data retention requirement would threaten privacy in a number of ways.

Such a requirement would require the storage of massive volumes of data by a wide range of organisations with widely-varying degrees of sophistication and resources and therefore poses very significant security risks. With reports of significant data breaches occurring on an almost daily basis, and suspicions that there are have also been a large number of data breaches that have not been reported[1], the likelihood that the data retained under such a requirement would be compromised is all but guaranteed.

Even if were to be specified that the actual content of communications is not to be retained, information such as addresses of websites visited, email addresses and phone numbers to which messages are sent to and received from, details of phone calls sent and received, and other online communications activities, along with associated dates, times and locations does amount, in many cases to content and is highly personal data.

A URL (website address) will in many instances allow for the content of that website to be accessed well after the fact, providing a direct link to content. Many URLs also contain sensitive information, such as usernames and even passwords. Similarly, in the telephone context, while the actual phone number dialled may not be content, any numbers input after connection, in response to a phone tree or other verbal prompts (known as post cut through dialled digits, or PCTDD) are content. In many cases this content will be highly sensitive, including bank account or credit card numbers, dates of birth and PINs.

It has also been seen that the difficulty in segregating content from non-content can lead to over-retention. For example, email subject lines may be retained along with other header information, but they are clearly contents of communications.[2]

[1] http://www.oaic.gov.au/news/media_releases/media_release_120430_business-warned-to-be-ready.html
[2] See European Union, Article 29 Data Protection Working Party, Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation 9 (2010), available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf

While much data that would be retained would in isolation appear harmless, the aggregate of this data will reveal highly intimate details of a person's life. This would include religious and political affiliations, sexual orientation, health issues and other such highly-sensitive information. A very recent example from the United States, where the retail store Target analysed shopping histories to identify pregnant women, in order to send them highly-targeted offers, is a disturbing example of the potential for massive data sets to be exploited.

The consequences of a breach of such highly personal data could be catastrophic for the individuals affected, leading potentially to identity theft, relationship break-downs, loss of employment, public humiliation or worse. In the Target example referred to above, the father of a pregnant teenager was alerted to the fact of her pregnancy as a result of seeing the marketing offers sent to her in the mail.[3]

Telstra CEO David Thodey recognised this when he responded to a recent incident involving Telstra's harvesting of the URLs visited by customers of its NextG mobile service in order to provide this information to a foreign company. He is reported to have said in an internal email that "customer privacy is not negotiable"[4]. This incident also demonstrates the risk of misuse of data by organisations for their own internal marketing purposes, which is a serious likelihood as they will seek to offset the significant costs associated with maintaining storage facilities for such large volumes of data.

There is also a risk of employees accessing retained data for their own personal purposes, which could range from idle curiosity to stalking or other criminal activities.

Further, the existence of retained data could potentially make that data accessible to third parties through court orders and other legal proceedings.

In its decision striking down the German data retention law based on the European Data Retention Directive, Germany's Federal Constitutional Court noted:

> "Even though the storage does not extend to the contents of the communications, these data may be used to draw content-related conclusions that extend into the users' private sphere... The observation over time of recipient data, dates, times and the place of phone conversations, it continued, "permit detailed information to be obtained on social or political affiliations and on personal preferences, inclinations and weaknesses."[5]

While Australians enjoy no explicit legal or constitutional right to privacy, the reasonable expectation by Australians is that their daily lives, of which electronic communications form an increasing part, should be free from arbitrary interference or monitoring by government. EFA believes that most Australians would greet the proposed system with suspicion and alarm at the threat it poses to their privacy. This should also be a factor in any decision to legislate in this area.

Erosion of civil liberties

[3] http://afr.com/p/technology/big_data_creeps_out_online_customers_2CJAxqYONJO2wzf1Yos7YL
[4] http://www.itwire.com/business-it-news/security/55578-privacy-thodey-thumps-telstra-team-over-trust-breach
[5] http://www.bverfg.de/pressemitteilungen/bvg10-011en.html

The existence of large-scale databases of communication activity raises the potential for abuse by governments and police. While we can earnestly hope that sufficient checks and balances would exist to prevent authorities abusing such databases to gather information on protesters (for instance), the only way to ensure that this never happens is to prevent the data being collected in the first place.

Germany's Federal Constitutional Court also addressed this issue:

> "Depending on the use of the telecommunication, such storage can make it possible to create meaningful personality profiles of virtually all citizens and track their movements. It also increases the risk of citizens to be exposed to further investigations without themselves having given occasion for this. In addition, the possibilities of abuse that are associated with such a collection of data aggravate its burdensome effect. In particular since the storage and use of data are not noticed, the storage of telecommunications traffic data without occasion is capable of creating a diffusely threatening feeling of being watched which can impair a free exercise of fundamental rights in many areas."[6]

Potential for scope creep

EFA is also concerned that should such a system be put in place, the scope of acceptable uses would be too broad or would be broadened in response to political pressure. This could lead to retained data being used for unfocused 'fishing expeditions' by law enforcement, or for it to be made available for use in civil proceedings relating to alleged copyright infringement, or other matters.

Costs to service providers

A blanket data retention requirement would impose a significant cost burden on communications companies including retail internet service providers. ISPs log certain types of data as part of their normal operations and for the purposes of billing or providing other services. However, maintaining records of all accessible data for long periods of time, as well as servicing law enforcement requests to access the data, would impose costs far above those of normal operations.

According to the UK Internet Service Providers' Association one large UK-based ISP estimated that it would cost £26m a year to set up a data retention system along with £9m a year in running costs.[7] These are costs that would inevitably be passed directly on to Australian businesses and consumers in the form of higher connectivity and other service charges.

These additional costs could also lead to a reduction in competition, as they will disproportionately affect smaller providers.

International context

The European Union's data retention regime was set in place with the adoption of the aforementioned Data Retention Directive (2006/24/EC), on "the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC".

[6] http://www.bverfg.de/pressemitteilungen/bvg10-011en.html
[7] http://www.theregister.co.uk/2005/12/14/eu_data_retention_vote/

The Directive covers fixed, mobile and internet telephony and Internet access and email communications. Member states are required to craft legislation that mandates the retention for between 6 months and 2 years of enough information to determine the type, location, time, duration and destination of a communication. This amounts to enormous volumes of data.

Courts in a number of European Union countries have already ruled that national data retention laws based on the Directive are unconstitutional. These countries include:

- Germany[8]
- Czech Republic[9]
- Cyprus[10]
- Bulgaria[11]
- Romania[12]

Constitutional challenges to data retention laws are also underway in other European Union countries, and a court in Ireland has referred a data retention case to the European Court of Justice and questioned the legality of the entire EU Data Retention Directive.[13]

Senate Environment and Communications Reference Committee inquiry

EFA reminds the Committee of the recent inquiry performed by the Senate Environment and Communications Reference Committee (the SECRC) into data retention proposals, as part of their consideration of the adequacy of protections for the privacy of Australians online[14].

The SECRC commented in their report that:

> "The committee's central concerns about the proposal are the very real possibilities that it is unnecessary, will not provide sufficient benefit to law enforcement agencies, and is disproportionate to the end sought to be achieved. The proposal has very serious privacy implications, even if one accepts the arguments of the Attorney-General's Department and AFP that the same information is already available for fixed-line telephone records. The fact is that much of the information intended to form part of the scheme does not need to be collected for any other purpose, so the only reason to retain it is the mere possibility that it may prove useful to law enforcement. This seems to the committee to be a significant departure from the core principles underpinning Australia's privacy regulation." [15]

And continued,

[8] http://www.edri.org/edrigram/number8.5/german-decision-data-retention-unconstitutional
[9] http://husovec.blogspot.com/2012/01/czech-constitutional-court-gives.html
[10] http://edri.org/edrigram/number9.3/data-retention-un-lawful-cyprus
[11] http://edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention
[12] http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf
[13] http://edri.org/edrigram/number8.10/data-retention-ireland-ecj
[14] http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=ec_ctte/online_privacy/index.htm
[15] http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=ec_ctte/online_privacy/report/c04.htm#anc5

> "Furthermore, the committee considers that there is a very real risk that the most serious, tech-savvy criminals—particularly those involved in fraud and child pornography—will be able to evade monitoring in any respect as a result of technological developments. "[16]

The recommendations included in the SECRC report are that, before the Government pursue any mandatory data retention program, it must:

- undertake an extensive analysis of the costs, benefits and risks of such a scheme;
- justify the collection and retention of personal data by demonstrating the necessity of that data to law enforcement activities;
- quantify and justify the expense to Internet Service Providers of data collection and storage by demonstrating the utility of the data retained to law enforcement;
- assure Australians that data retained under any such scheme will be subject to appropriate accountability and monitoring mechanisms, and will be stored securely; and
- consult with a range of stakeholders.[17]

In the Discussion Paper issued to the Joint Committee on Intelligence and Security (JCIS), the Attorney-General's Department has not addressed these concerns of the SECRC. The Department has rather provided Parliament with a second vaguely-defined and inadequately-justified data retention proposal.

EFA recommends that JCIS should require the Attorney-General's department to address all of the concerns raised by the SECRC before considering the issue of mandatory data retention. At the very least, the Department should conduct broad consultations, provide a concrete proposal, and undertake a cost-benefit analysis.

Conclusion

EFA believes that the introduction of a data retention requirement would amount to an unprecedented invasion of the privacy and curtailment of the civil liberties of all Australians.

It would lead to the collection of enormous volumes of extremely sensitive personal data involving every resident of and visitor to Australia. This data could (and almost certainly would) be exposed accidentally or maliciously and would be open to abuse by private individuals, law enforcement and governments.

The existence of such a requirement could also have a corrosive effect on Australians' faith and trust in government, a chilling effect on freedom of expression and potentially even a negative impact on internet usage within Australia.

EFA believes that any data retention requirement must be tightly constrained in order to safeguard the privacy of Australians' communications, as follows:

- Very short horizons for expiry of data

16 http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=ec_ctte/online_privacy/report/c04.htm#anc5

17 http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=ec_ctte/online_privacy/report/c04.htm#anc5

- Strict restrictions on access, and access only under judicial order
- Exclusion of data that is part of the contents of communications (such as an email subject line)
- Strict limits on the protocols and data covered by the requirement to those with a demonstrated use in prosecution of serious crimes, not a blanket mandate to ISPs to save “all logged data".
- Exclusion of email communications, at the very least unless the service provider is the primary host of the email accounts in question
- Exclusion of web-browsing histories
- Prohibition on the use of any retained data for civil purposes, such as copyright enforcement
- Strict requirements for the secure destruction of retained data after the expiry of the retention period

Extending the scope of surveillance

The Discussion Paper contains three proposals that, when combined, represent an over-reaching but worryingly vague extension of surveillance powers in relation to distributed computing and social network services. They combine to allow a surveillance reach so broad as to cover all spheres of life and indirectly creating an inherent system of collateral surveillance of all Australians. These three proposals are detailed below.

1. Relevant Act: *Telecommunications (Interception and Access) Act 1979*

Terms of Reference extract:
9. Modernising the Industry assistance framework –
a. extend the regulatory regime to ancillary service providers not currently covered by the legislation

2. Relevant Act: *Telecommunications Act 1997*

Terms of Reference extract:
16. Amending the Telecommunications Act to address security and resilience risks posed to the telecommunications sector. This would be achieved by:
b. by instituting obligations to provide Government with information on significant business and procurement decisions and network designs

3. Relevant Act: *Australian Security Intelligence Organisation Act 1979*

Terms of Reference extract:
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.”

Submission

While EFA recognises the manner in which these proposals represent important updates to legacy surveillance, from the civil liberties perspective of Australian individuals, each proposal comes with significant concerns, as outlined below.

Proposals 9.a. and 17.a.
As the Discussion Paper illustrates (p.18-19), communication increasingly involves a combination of mobile, distributed, and social network services. "Social Networking" and "cloud computing" are named as two examples of modern communication not currently intercepted that may create "vulnerabilities in the interception regime that are capable of being manipulated by criminals" (p.27).

EFA is concerned that:

(a) the Discussion Paper is in effect proposing surveillance of virtually unlimited services;
(b) that the Government is taking advantage of the concept of sharing in social networks, and
(c) that in so doing there is significant possibility for collateral surveillance of non-targeted individuals (and hence associated privacy risks).

The Discussion Paper claims that collateral surveillance could be reduced with "a simplified warrant regime that focuses on better targeting the characteristics of a communication that enable it to be isolated from communications that are not of interest." EFA is unconvinced that such a scheme is indeed possible.

Central to many of the services that Australians deliberately sign-up for— eg Facebook, Twitter, Pinterest, Apple iCloud, etc.—is the concept of sharing across networks. In surveilling a target's activities in such services, shared friends or media objects connect target and non-target individuals such that following one surveillance target inescapably involves collateral surveillance necessarily breaching the privacy of non-targets. While using such services do involve Australians' agreeing to the sharing of some information with the service operator, and Australians want to share some information with various known and unknown networks, the Government should not take advantage of this fact to breach individual privacy in the name of national security.

Further, underlying many social network services are distributed transmission and storage services both directly and indirectly related to the service in use (e.g. image caching, metric reporting etc). Indeed, "cloud computing" itself underlies "social networking". As such, the information flows pertaining to individuals cross and recross such services to the point where, again, separating surveillance of a particular target is almost inevitably going to encounter that of other individuals, but in this case in ways that cannot be anticipated and very deeply undermine Australians' reasonable expectation of privacy.

EFA recognises that the simplified warrant proposals do nod towards more sophisticated methods of pinpointing target communication and reducing the privacy invasion of collateral surveillance, but strongly recommends that any regulations expanding surveillance to non-C/CSPs provide extensive accounts for maximising the privacy of non-target individuals.

Proposal 16.b. "instituting obligations to provide Government with information on significant business and procurement decisions and network designs".
The Discussion paper frames the proposal of standardised tiered regulation in terms of protecting "infrastructure and the information held on it or passing across it from unauthorised interference to support the confidentiality, integrity and availability of Australia's national telecommunications infrastructure" (p.33). The desired method of regulation is "an approach that avoids the need for

government approval of network architecture at a technical or engineering level and instead focuses on the security outcome, leaving industry to choose the most effective way to achieve it" (p.35).

EFA is concerned that, while couched in terms of protecting the information, transmission, and storage of Australians' information, in the light of Proposal 9.a., Proposal 16.b. might be used to (a) pressure C/CSP and non-C/CSP services for unlimited 'backdoor' access (a single point of government access that bypasses all normal authentication) and/or (b) allow the circumvention of warrants for particular target individuals by instead claiming a national security need to surveil all or part of the operations of a C/CSP or non-C/CSP service.

EFA recognises that the tiered regulation proposal has a goal of reducing onerous constraints on the telecommunications industry, but recommends that any regulatory regime for industry cooperation with surveillance specifically rules out backdoor access and includes reference to a strict system of target warrants while ruling out unilateral national security claims.

Record-keeping and oversight

Relevant Act: *Telecommunications (Interception and Access) Act 1979*

Terms of Reference extract:
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:

- *c. mandatory record-keeping standards*
- *d. oversight arrangements by the Commonwealth and State Ombudsmen*

Submission

EFA is very concerned that this proposal seeks to replace existing mandated record-keeping requirements and to give each agency the 'flexibility' to determine their own record-keeping and reporting requirements.

Statistics from the United States show that the risk of agencies overstepping their authority is all too real. The Inspector-General of the United States Department of Justice recently found that the Federal Bureau of Investigation had used covert National Security Letters to issue thousands of improper record requests.[18] Between 2001 and 2008, it is estimated that as many as 40,000 violations of law, Executive Order or other regulations governing intelligence investigations were committed by the FBI.[19] In response to these violations, the Inspector-General recommended that record-keeping requirements be imposed on the FBI that are of a very similar nature to those that this proposal seeks to remove.[20]

The discussion paper suggests that the current record-keeping arrangements should be modified as they "reflect historical concerns about corruption and the misuse of covert powers." (p.26) EFA

[18] Office of the Inspector General, U.S. Department of Justice, *A Review of the FBI's Use of NationalSecurity Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006* (2008), available at: http://www.justice.gov/oig/special/s0803b/final.pdf .
[19] See Electronic Frontier Foundation, Patterns of Misconduct: FBI Intelligence Violations from 2001-2008 (2011), available at: https://www.eff.org/pages/patterns-misconduct-fbi-intelligenceviolations
[20] See OIG, Review of the FBI's Use of National Security Letters, supra note 23, at 14-33.

rejects the assertion that concerns about corruption and the misuse of covert powers are somehow no longer valid. In the context of a range of proposals that seek to massively expand the scope of surveillance powers, this assertion seems to be an example of Orwellian doublespeak.

Given the general lack of transparency that is inherent with intelligence and law enforcement agencies, it is imperative that independently-vetted record-keeping and reporting requirements are imposed to minimise abuse of power and to ensure effective oversight by Ombudsmen and other review agencies. EFA therefore calls on the Committee to reject this proposal.

Extension of warrants

Relevant Act: *Australian Security Intelligence Organisation Act 1979*

Terms of Reference extract:
5. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions
   a. 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.

Submission
EFA believes that there is no justification for amending the ASIO Act to allow the Attorney-General to double the validity period of warrants. A 90 day period is already very significant, and the Act already provides the ability for 'further warrants' to be issued after the expiration of that period. Where the circumstances justifying the warrant have not changed, it would not represent a significant administrative burden for a further warrant to be applied for, as the underlying information would be the same.

EFA believes that simple administrative convenience is not a sufficient justification for the reduction in independent oversight that would result from this proposed amendment and therefore recommends that the Committee should reject this proposal.

Standardisation of warrant tests and thresholds

Relevant Act: *Telecommunications (Interception and Access) Act 1979*

Terms of Reference extract:
2. Reforming the lawful access to communications regime. This would include:
   a. the standardisation of warrant tests and thresholds

Submission
EFA understands that there may be administrative benefits arising from a standardisation of warrant tests and thresholds between both content and stored communications warrants, but is unconvinced that reducing the threshold of what constitutes a 'serious offence' in this context from an offence carrying a penalty of 7 years, to one carrying a penalty of 3 years, is justified. EFA is very concerned that telecommunications-related offences might be planned to have incommensurately high sentences so that they fall under conditions for relevant warrants.

EFA therefore recommends that the Committee reject this proposal.

Criminalisation of failure to assist in decryption

Relevant Act: *Telecommunications (Interception and Access) Act 1979*

Terms of Reference extract:
15. Modernising the Industry assistance framework
a. establish an offence for failure to assist in the decryption of communications

Submission
Encryption is an important data security measure that is routinely used as part of entirely legitimate activities to prevent unauthorised access to sensitive and important data. Encryption is of course also used by persons planning or undertaking criminal activities.

EFA is concerned about the possible creation of an offence for failing to assist in the decryption of communications for the following reasons:

1. it undermines the right of individuals to not cooperate with an investigation
2. it poses a threat to the independence of journalists and their sources, particularly in circumstances involving whistle-blowing activity related to cases of official corruption
3. it could undermine the principles of doctor-patient and lawyer-client confidentiality and other trusted relationships
4. there are foreseeable and entirely legitimate circumstances in which decryption of data is not possible, such as where a password has been forgotten and is unrecoverable.

EFA therefore believes that the Committee should reject this proposal.

Tampering with computers

Relevant Act: *Australian Security Intelligence Organisation Act 1979*

Terms of Reference extract:
11. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions to:
a. Enable the disruption of a target computer for the purposes of a computer access warrant

Submission
EFA is gravely concerned about this proposal. The proposal that ASIO would be permitted to 'add, delete or alter data or interfere with, interrupt, or obstruct the lawful use of a computer' could lead to some very serious consequences. These could include:

- pollution of evidence, potentially leading to failures of convictions
- providing the means for evidence to be 'planted' on innocent parties, thereby potentially leading to miscarriages of justice
- serious disruption to lawful business and other activities, amounting to significant economic loss, including to entirely unrelated persons and organisations in the case of shared computing resources (such as a shared webhosting server, many of which provide services to hundreds, if not thousands of different customers)

EFA therefore strongly recommends that the Committee reject this proposal.