Submission No 165

Inquiry into potential reforms of National Security Legislation

Organisation: Blueprint for Free Speech

blueprint for
FREE SPEECH

Submission

to the JCIS Inquiry into Potential Reforms of National Security Legislation

MELBOURNE, AUGUST 2012

blueprint for
FREE SPEECH

PO Box 187, Fitzroy VIC 3065
247 Flinders Lane, Melbourne VIC 3000
info@blueprintforfreespeech.net

blueprint for FREE SPEECH

PO Box 187, Fitzroy VIC 3065
247 Flinders Lane, Melbourne VIC 3000
info@blueprintforfreespeech.net

Submission to the JCIS Inquiry into Potential Reforms of National Security Legislation

Summary

Thank you for the opportunity to provide comments on *Equipping Australia against Emerging and Evolving Threats* (the **Discussion Paper**). We are a non-profit organization concerned with matters around each individual's right to freedom of expression. Part of freedom of expression is the individual's right to determine the manner in which they communicate. In other words, it is to determine whom they wish to communicate with and when they wish to stop that communication or to delete it. We argue that human rights, individual privacy, and proportionality should also be paramount considerations in any reform of Australia's national security legislation in the area of telecommunications. It is pleasing that those ideals are articulated in the Terms of Reference for the Inquiry.[1] However, we believe the proposed reforms would fall far short of achieving them.

We object to the proposals in the Discussion Paper on the grounds that:

- they would unreasonably interfere with people's privacy;
- they would have a chilling effect on freedom of expression;
- they would impose unreasonable costs and an inappropriate role on the telecommunications industry, and this cost would likely be passed onto consumers;
- they do not account for the possible misuse of powers and provide inadequate countervailing protections of privacy;
- they would dramatically and unnecessarily expand ASIO's powers;
- it has not been adequately demonstrated to the public that reforms are necessary;
- it has not been adequately demonstrated to the public that the reforms would achieve their declared objectives; and
- the Discussion Paper is extremely vague about many details of the reforms, particularly those that will have serious impacts on privacy and freedom of expression.

[1] Discussion Paper, 6.

PO Box 187, Fitzroy VIC 3065
247 Flinders Lane, Melbourne VIC 3000
info@blueprintforfreespeech.net

Australia is a representative democracy that prides itself on offering great freedom to its citizens. One aspect of this freedom is the right to free speech. Another is the right to individual privacy, from government and other citizens. Over the past ten years, both rights have been significantly eroded in Australia in the name of national security. This trend should be reversed, not expanded.

Finally we note that although there has been an extension to the deadline for submissions to regarding this report, the initial timeline was exceedingly short. In future we believe it necessary for a submission period of at least 6 and preferably 8 weeks to be given to the broader community to prepare and make submissions on such a complex area of law. Such lead times are necessary in order that those in the community who are interested can learn about the submission process, analyse the proposals and develop a response.

Information interception

1 The rationale for reform

The Discussion Paper assumes that reforms to the information interception regime are necessary without adequately establishing why. It asserts that the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**) 'reflects the use of telecommunications and the structure of the telecommunications industry that existed in 1979 when the Act was made' and that 'urgent reform' is therefore needed.[2] However, little evidence is given to establish that the 'legacy assumptions' the TIA Act is supposedly based on are truly problematic.[3] Law enforcement agencies (and presumably also ASIO) continue to use telecommunications interception regularly and with high levels of success.[4] Indeed, data released by the Government shows that agencies access electronic data at an astonishing rate, with 250,000 separate instances occurring in 2010–2011.[5] This suggests two things. First, the current scheme is not fundamentally unworkable. Secondly, if anything Australian agencies have too much power to access electronic communications, not too little.

---

[2] Discussion Paper, 12.

[3] Discussion Paper, 20.

[4] Discussion Paper, 14.

[5] Philip Dorling, 'Police spy on web, phone usage with no warrants', *Sydney Morning Herald* (18 February 2012) <http://www.smh.com.au/technology/technology-news/police-spy-on-web-phone-usage-with-no-warrants-20120217-1tegl.html>.

PO Box 187, Fitzroy VIC 3065
247 Flinders Lane, Melbourne VIC 3000
info@blueprintforfreespeech.net

The TIA Act has been amended many times since it was enacted, particularly in the last 10 years.[6] The Discussion Paper acknowledges this, but instead of acknowledging that the Act has been progressively modernised, it is cited as a further reason to amend the Act on the basis that it has become too complex.[7] This raises questions about the rationale for the reforms and their objectives. Is the TIA Act obsolete, or has it been updated too frequently? Are the reforms directed at clarifying the law, or achieving a wholesale overhaul? The Discussion Paper is conflicted and unclear on these critical issues.

In our view, the burden is on the Government to demonstrate to the public that wide-ranging reform of Australia's telecommunications interception rules is needed. On critical issues of national concern such as these, all policymaking should be based on extensive evidence. None has been provided and the case for reform has not been made out.

2 Privacy and abuse of powers

We agree that it would be helpful to strengthen the language of the objects clause of the TIA Act to better promote the protection of privacy as an object of the Act. However, objects clauses provide a gloss on legislation, but are not strong safeguards against abuse. Particularly in the context of the TIA Act, which confers broad discretionary powers, a modified objects clause would not provide sufficient protection against inappropriate incursions on privacy.

The Discussion Paper does not take into account the possibility that the powers it proposes could be abused. It states:

> The requirements are aimed at ensuring that agencies keep appropriate records necessary to demonstrate that agencies are using their powers lawfully. However, many of the requirements reflect historical concerns about corruption and the misuse of covert powers and do not reflect the current governance and accountability frameworks within which agencies operate.[8]

---

[6] See TIA Act, Table of Amendments.

[7] Discussion Paper, 17.

[8] Discussion Paper, 26.

PO Box 187, Fitzroy VIC 3065
247 Flinders Lane, Melbourne VIC 3000
info@blueprintforfreespeech.net

It is difficult to tell exactly what this statement means. However, a fair reading is that it rejects the possibility that covert powers could be abused. That is a serious mistake: the potential for abuse should *always* be kept in mind. Further, it is very difficult to understand how reducing record-keeping requirements would contribute to transparent, high-quality decision-making.

Information security and access to data by government

1 Protection of data by service providers

In line with our belief in the importance of individual freedom to determine who should or should not be party to their communications and speech, we support the introduction of an obligation on telecommunications service providers to ensure their networks are secure. However, the way in which the Discussion Paper proposes to achieve this is highly problematic.

The Discussion Paper argues that service providers should be required to protect 'sensitive, private or classified information for the purpose of espionage, political, diplomatic or commercial advantage'.[9] In our view, it is completely inappropriate for service providers to be given that role. They are not equipped to judge whether information falls within those categories and it would be very expensive and impractical to require them to make such assessments.

More importantly, service providers should not be turned into proxy police. It is not their role to analyse information to determine whether it is significant for national security. The imposition of such a role would be a major incursion on the privacy of those who use service providers — which is virtually everyone. Moreover, the costs of the requirements would inevitably be passed on to clients. This means the public would effectively be paying to have their privacy invaded.

There is also a balance to be struck between privacy and freedom of information. The proposals could unduly restrict the latter by requiring service providers, for example, to restrict access to 'sensitive' information for 'political' reasons.[10] This is too broad and would effectively prevent people from viewing information they are perfectly entitled to access.

---

[9] Discussion Paper, 32.

[10] Discussion Paper, 15.

PO Box 187, Fitzroy VIC 3065
247 Flinders Lane, Melbourne VIC 3000
info@blueprintforfreespeech.net

2 Information sharing with government

Privacy means not only the right to expect that information will not be shared with other individuals and private organizations, but also that it will not be shared with government without good reason. In addition to suggesting very strong protections on information in the form of requirements on service providers, the Discussion Paper also proposes:

> a requirement for C/CSPs to provide Government, when requested, with information to assist in the assessment of national security risks to telecommunications infrastructure;[11]

There is a certain irony in this. What is being proposed is that service providers should implement very strong protections against *private* access to private information. But that same information, or at least a part of it, must be shared with the Government to assist with national security assessments. In our view, this is not a balanced way to approach data security. Australians expect their data to be secure from intrusion by anyone, including the Government.

The Discussion Paper also fails to spell out any real limits on what the Government may do with information once it has received it. Increasingly, governments around the world, including the Australian Government, are sharing large volumes of citizens' personal data with each other in the name of national security.[12] This is very concerning as the arrangements of the sharing have rarely if at all been open to public debate and scrutiny. This is a data sovereignty issue and as such deserves the highest level of transparency to the citizenry to determine if they support their communications and data (their 'speech') being sent to foreign powers, and under what circumstances.

3 Data retention

---

[11] Discussion Paper, 34.

[12] For recent agreements providing for the sharing of passenger data, see: *Agreement between the European Union and Australia on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the Australian Customs and Border Protection Service* [2012] ATS 19; *Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security* (8 December 2011) <http://register.consilium.europa.eu/pdf/en/11/st17/st17434.en11.pdf>.

PO Box 187, Fitzroy VIC 3065
247 Flinders Lane, Melbourne VIC 3000
info@blueprintforfreespeech.net

We are extremely concerned about the proposal to require service providers to retain data for two years. If implemented, this measure would dramatically reduce privacy in Australia, with very few demonstrated national security benefits. It would also have a serious effect on freedom of speech.

People have a legitimate expectation that when they delete electronic information, it is gone. They do not expect their service provider to secretly retain it against their wishes. The proposal is analogous to secretly collecting everyone's garbage for two years and storing it in case it might assist a criminal investigation at some point in the future. In addition, it effectively prevents people from deleting their information, which is analogous to passing a law making it illegal to destroy your own documents. If this proposal were not in the digital sphere, it would never be accepted. It should not be accepted for online content. We note that methods and policies for eventual deletion of the stored data after the retention period are not specified.

Further, we do not believe service providers are appropriate depositories for people's data even if it is to be retained. They are not adequately equipped to protect large quantities of information, as recent high profile instances of hacking demonstrate.[13] Imposing an obligation on service providers to protect data is not an adequate solution to this problem. If anyone is going to keep data for government purposes — and we do not believe anyone should — it should be the Government, not the private sector, and appropriate constraints on its storage, access and disposal must be put in place. However we reiterate that we strongly oppose such a proposal for retaining the data in the first place, and based on recent media, our views appear to be in line with public attitudes to the matter.

There is no evidence to suggest data retention would assist with the prevention of crime or terrorism. A 2011 study of Germany's Data Retention Directive found it had no impact on either the effectiveness of criminal investigations or the crime rate. Further, the study specifically found that countries *without* data retention laws are not more vulnerable to crime:

---

[13] See, eg, Andrew Colley, 'AAPT hack by Anonymous poses crime data leak fears for AFP and ACC', *The Australian* (31 July 2012) <http://www.theaustralian.com.au/australian-it/government/aapt-hack-by-anonymous-poses-crime-data-leak-fears-for-afp-and-acc/story-fn4htb9o-1226439504262>.

PO Box 187, Fitzroy VIC 3065
247 Flinders Lane, Melbourne VIC 3000
info@blueprintforfreespeech.net

> There is no proof that the number of cleared cases, the crime rate or the number of convictions, acquittals or closed cases significantly depends on whether a blanket data retention scheme is in operation in a given country or not. There is no evidence that countries using targeted investigation techniques clear less crime or suffer from more criminal acts than countries operating a blanket communications data retention scheme.[14]

In 2010, Germany's Constitutional Court struck down the Directive, calling it a 'particularly serious infringement of privacy in telecommunications' that did not adequately protect users' information and subverted the public's legitimate expectation of privacy.[15] The proposed Australian measure would suffer from the same defects and should not be adopted.

Warrants, ASIO powers and decryption assistance

1 Changes to the warrant regime

The Discussion Paper proposes '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.'[16] Although little detail is given about this proposal, it appears to focus on the content of communications rather than who sends them. This raises serious issues about unjustified invasions of privacy. Moreover, the proposals have to be seen in the context of significant recent expansions of powers for national security agencies such as ASIO. In our view, those powers should be limited rather than expanded.[17] As the Discussion Paper recognises, there have only been 22 terrorism-related convictions in Australia in the past decade.[18] While we acknowledge that terrorism is a serious problem, it is important that measures intended to combat it do not end up undermining the basic freedoms Australians expect to enjoy.

---

[14] Arbeitskreis Vorratsdatenspeicherung, *Serious criminal offences, as defined in sect. 100a StPO, in Germany according to police crime statistics* (19 February 2011) <http://www.vorratsdatenspeicherung.de/images/data_retention_effectiveness_report_2011-01-26.pdf>.

[15] BBC Online, *German court orders stored telecoms data deletion* (2 March 2010) <http://news.bbc.co.uk/2/hi/europe/8545772.stm>

[16] Discussion Paper, 25.

[17] See, eg, *Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003* (Cth); *Anti-People Smuggling and Other Measures Act 2010* (Cth) sch 3; *Intelligence Services Amendment Act 2011* (Cth).

[18] Discussion Paper, 15.

PO Box 187, Fitzroy VIC 3065
247 Flinders Lane, Melbourne VIC 3000
info@blueprintforfreespeech.net

Warrants based on the content or characteristics of communications are more likely to be excessively broad and open to abuse than personal warrants. For one thing, the agency would have to sort through many communications to determine whether they were 'of interest'. This in itself would be a serious invasion of privacy, even if the communications were not used. Privacy means that your data is safe from prying eyes, not just that it is safe from misuse. In addition, warrants of this kind would be more likely to authorise fishing expeditions by agencies because it is largely up to the agencies themselves to define what is or is not 'of interest' to an investigation. Therefore, the scope of the warrants would be largely self-defining.

2 The introduction of special advocates

Instead of broadening the powers of ASIO and other law enforcement agencies, we believe the warrant system should be modified so that *special advocates* are employed to oppose warrant applications. Currently, ASIO makes warrant applications to the Attorney-General *ex parte*, with no opportunity for an opposing view to be argued. Although we understand there may be a need for secrecy in respect of some ASIO warrants, the deployment of special advocates would create a balanced and just process to the extent possible. It is important that they be independent and not based in the Attorney-General's Department; in our view, it would be appropriate for them to work from the Office of the Australian Privacy Commissioner. Further, their security clearances should be arranged and reviewed by a method not dependent on ASIO. This is to ensure that the public could have confidence that the advocates are truly independent, free from any possible internal pressure from the security agencies. However, it would be appropriate if the funding for the special advocates came from ASIO's budget as their role is to ensure the lawfulness and proportionality of a process ASIO initiates for its own purposes.

Such advocates would study the same material available to ASIO or other agencies, and then make the case as to why a citizen's privacy should not be breached by the state, or in the case of a renewal to a warrant, continue to be breached by the state. This would be provided to the deciding authority, such as the Attorney General or in the case of other possible warrants, to a judge.

In this manner, the decision maker would hear arguments from representatives of both the State and the individual citizen (by proxy) as to why the balance of rights between the two should be

PO Box 187, Fitzroy VIC 3065
247 Flinders Lane, Melbourne VIC 3000
info@blueprintforfreespeech.net

changed. Thus the decision maker would be able to make thoroughly informed choices regarding the State's request to take away the privacy enjoyed by its citizens.

The citizens' advocate would not need to be in contact with the citizen nor to seek their views where secrecy is required. As long as their role was clear, this lack of contact should not be a barrier.

3 Modifying data and controlling computers

The proposals in the Discussion Paper to allow ASIO to modify the data on computers and use third-party computers as a means to intercept communications are highly inappropriate. No reasons are advanced why these powers might be necessary. An assertion that they would be convenient for ASIO is all that is provided.

Measures of this kind raise clear questions about privacy and human rights. It is difficult to conceive of an invasion of privacy more serious than modifying the contents of a person's computer — for example, by deleting content on it or adding files that may be incriminating. Actions of this kind could so easily be abused that they should not be considered unless there is a seriously compelling reason to allow them. No reason has been advanced.

Allowing the computers of innocent third parties to be covertly used to infiltrate a target is equally reprehensible. Ordinary Australians would never expect their computers to be used for this purpose, and in our view they would not agree to it if asked.

The only mechanism proposed to control the proposed new powers is a proportionality test. That is simply not sufficient to ensure they are not misused. In the vast majority of cases, the people affected by actions of this kind would never know they had occurred, so they would not be challenged. To make the power subject only to a proportionality test — which would essentially require only that the agency in question believed the incursion was reasonable — would do little to prevent misuse because it would rarely be challenged in court.

Of most concern, however, is the cavalier way these proposals have been inserted in the Discussion Paper with very little in the way of details or justification. Again, we express our firm

PO Box 187, Fitzroy VIC 3065
247 Flinders Lane, Melbourne VIC 3000
info@blueprintforfreespeech.net

belief that the onus is on the Government to demonstrate that measures of this kind are absolutely necessary. That has not been done.

4 Decryption assistance

Although no details are given, the Discussion Paper proposes the creation of an 'offence for failure to assist in the decryption of communications'. We note, first of all, that password offences of this kind already exist in s 3LA of the *Crimes Act 1914* (Cth) and s 201A of the *Customs Act 1901* (Cth). These offences allow authorities to seek an order from a Magistrate requiring a person to provide assistance in accessing protected data. Therefore, there is no need for a new provision of this kind. We certainly would not support any similar provision that removed the requirement to obtain an order from a judicial authority.

More importantly, any offence of this kind is seriously problematic and contrary to fundamental principles. In the first place, it is manifestly inconsistent with the right to avoid self-incrimination. It is also attended by a range of other problems that could lead to serious injustice.

An offence of this kind risks punishing people for their state of mind. For example, the inability to remember a password could lead to a conviction. Further, it is difficult to see how encrypted documents could be infallibly identified. An encrypted document is merely a jumble of letters and characters with no sequences or other indications of its content. It is difficult or impossible to separate such documents from those which are not encrypted but happen to consist of random characters. A person could be convicted of the offence merely for having such a document if they could not prove it was *not* encrypted — an Orwellian scenario that clearly involves a reversal of the burden of criminal proof. Finally, if the offence were conditional on the person *successfully* decrypting the document, they could be convicted even if they gave their password up if the document was encrypted by a group of people each with an individual password, all of which was required for decryption.

These scenarios demonstrate that an offence of this kind should not be adopted. There is no demonstrated need for it and the risks it brings of injustice and abuse are too great.

PO Box 187, Fitzroy VIC 3065
247 Flinders Lane, Melbourne VIC 3000
info@blueprintforfreespeech.net

Conclusion

Freedom of expression and the related right to keep some things private are central to the functioning of democracy in Australia. The trend in the last decade has been to limit both in favour of an expansion in power of Australian security agencies. It does not have to be that way. Freedom of speech and privacy can and should be protected regardless of other imperatives. There is no need to interfere with them to achieve security.

Even if we accept the view that there is a push and pull between freedom of speech and privacy and the power of Australia security agencies, the proportionality of those values is barely touched upon in the Discussion Paper. The government is simply taking fruit from the 'freedoms' basket and placing it in the 'national security' basket without demonstrating why.

The Government has released a Discussion Paper, but really it is not yet a discussion: the onus is on the government to make a basic factual case about why reform is needed. Only then will the public be able to adequately defend its right to freedom of expression and privacy.