Blueprint for Free Speech

Submission to:

Parliamentary Joint Committee on Intelligence and Security in respect of the National Security Legislation Amendment Bill (No. 1) 2014

6 August 2014

Submission to the Parliamentary Joint Committee on Intelligence and Security (the Committee) in respect of the National Security Legislation Amendment Bill (No. 1) 2014 (the Inquiry).

6 August 2014

1 Introduction

Thank you for the opportunity to provide comments to the Committee in respect of the Inquiry.

Blueprint for Free Speech (**Blueprint**) is an Australian based, internationally focused not-for-profit concentrating on research into 'freedoms' law. Our areas of research include public interest disclosure (whistleblowing), freedom of speech, defamation, censorship, right to publish, shield laws, media law, Internet freedom (net neutrality), intellectual property and freedom of information. We have significant expertise in whistleblowing legislation around the world, with a database of analyses of more than 20 countries' whistleblowing laws, protections and gaps.

You may be aware that Blueprint contributed to the Parliamentary Joint Committee on Intelligence and Security's '*Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*', which reported in May 2013 (**PJCIS Report**). During this process, we provided a written submission, an oral submission to the committee in Sydney and supplementary submission providing information specifically on the efficacy of implementing a data retention regime (each a **PJCIS Submission**, together our **PJCIS Submissions**). Additionally, in February 2014 we submitted to the Legal and Constitutional Affairs References Committee's Inquiry into comprehensive revision of the *Telecommunications (Interception and Access) Act 1979* (Cth), which related to these issues, and the PJCIS Report's recommendations.

This Bill was introduced on 16 July 2014 with the call for public comment by 30 July 2014. This was then extended until 6 August 2014. It is disappointing that for an issue of such magnitude only 14 days were initially given to the public and interested parties to prepare submissions in respect of the Bill. Although this was extended to 21 days, this period is still very short for legislation that runs to more than 100 pages in length. We sincerely hope that the Committee gives serious consideration to the public consultation process and casts a wide net when inviting experts to give oral submission to the committee before the Bill is again introduced to the parliament.

In light of the small window we have focused our written submission on what we consider to be the key issues of the Bill – those most concerning and in need of urgent re-consideration. We have set out these concerns below.

At the outset, we need to categorically state that journalism should not be a crime This law will make it one. A free media is essential for Australia to be a transparent and open democracy. Every Australian should reject the section of the bill that turns the job of journalism into a criminal act with penalties up to 10 years in prison.

The same penalty will apply for disclosure to an MP who then discusses that disclosure with anyone else. If for example the information revealed a crime being committed and the MP needed to seek advice from an advisor, a lawyer, a fellow member of parliament or to engage in the public debate that would make the MP a criminal facing up to 10 years in prison - irrespective of the public interest nature of the disclosure. The Bill, as well as effectively criminalising journalism, criminalises the very function of a member of parliament – to represent, inform and serve the people who elected them. Should they try to perform that function by discussing an SIO, they may face up to 10 years in prison.

Further, this law will create two classes of Australians: those who have to obey the law and those who do not. This is fundamentally un-Australian. ASIO agents should not be allowed to lie to Parliament and our courts, nor to conduct fraud – yet this law would let them do so with impunity. The test the agent must meet is that "*any unlawful conduct involved in conducting the special intelligence operation will be limited to the maximum extent consistent with conducting an effective special intelligence operation*"[1] It is easy to imagine that lying on the public record might be justified by this provision. These are just some of the examples of what this new law would enable. Existing laws already provide special powers to the intelligence community to invade citizens' privacy, search premises, and eavesdrop on conversations and more. Giving agents a free pass to break the law in all but three specified areas is dangerous to our open democracy whilst simultaneously removing accountability. It recalls the secret police state of Eastern Europe in the 1970s and 1980s, and must be rejected.

2 Executive Summary & Recommendations

Before we discuss each of the points in further detail, we have included an executive summary with our recommendations for your convenience:

a) Special intelligence operations create a substantial increase in power for ASIO and the absolving of civil and criminal liability for operatives are disproportionate to their necessity. Blueprint opposes creating a new class of operations; agents should not be above the law. The temptation for wrongdoing in such circumstances is very serious. However, if they are to be created than at the very least, the requirement on each occasion should be properly particularised with greater clarity (suggested working of which is set out below);

b) Criminalising legitimate public interest disclosure on both employees of ASIO and journalists is a backward step in democracy and transparency and amounts to criminalising journalism. If the information was passed to an MP and that MP disclosed the information outside of parliament it too would fall foul of the Bill. This criminalises an MP acting in their representative capacity. These new offences should be categorically removed from the Bill by deleting proposed section 35P of the Schedule 3 to the Bill;

c) Changing the definition of 'computer' to include a network of computers is a significant amplification of interception warrant powers and will lead to collateral damage and leaves open the potential for abuse. Further particularisation and specification is necessary (which is set out below);

[1] Proposed sect on 35C(2)(c) of Schedu e 3 of the B

d) Legitimising the disruption of computers (including those of non-targeted third parties) is a significant amplification of existing powers and as with (c) above, may lead to significant collateral damage (further particularisation on suggested limitations may be found below);

e) The amendments contained in the Bill should have a 'sunset clause' of 2 years, during which time the necessity and effectiveness of the provisions' impact on preventing serious crime and terrorism will be examined. If their effectiveness is not demonstrated in that time they should be automatically repealed, with the onus on the Attorney-General to establish this fact.

3 Creation of 'Special Intelligence Operations' ("SIOs")

Blueprint is opposed to the introduction of SIOs to the Bill. By its Schedule 3, the Bill proposes to introduce the concept of 'special intelligence operations' to the ASIO Act, a special class of intelligence operations, which essentially limit civil and criminal liability of a person engaged in such an operation. Paragraph 54 of the Explanatory Memorandum to the Bill ("**EM**") provides:

> *"Currently, some significant investigations either do not commence or are ceased due to the risk that an ASIO employee or ASIO affiliate, using the new terms in the Bill, could be exposed to criminal or civil liability."*

The provisions in Schedule 3 permit the Director-General or a Deputy-Director General of ASIO to authorise and define an SIO. The justification for such an introduction is that there are certain situations where, for example, ASIO officers infiltrate a criminal operation and for the avoidance of losing 'cover' they also engage in that criminal operation.

It is fit and proper that an agent of the State, even one under cover, should not engage in certain activities that are illegal (and presumably also unethical). There must be limits on actions, and there has been no proper argument or evidence presented in this draft legislation justifying such an expansion of powers. We have recently seen cases where these lines have been crossed. For example, in the UK a former undercover officer fathered a child with a woman unaware of his true identity.[2] In related cases, undercover officers duped women into sexual relationships – one of which lasted 6 years. These unethical behaviours – as part of undercover operations – are now rightly the subject of court cases. While the draft legislation does not create impunity for sexual offences, it is not clear the sort of unethical behaviour we have seen from undercover agents in the UK and which is clearly outside community standards in both the UK and Australia, would be prevented under this proposed legislation.

The second issue with this is that the definition of a 'special intelligence operation' is a discretionary power left in the hands of ASIO, with a potential duration of up to 12 months. Although the power to create a 'special intelligence operation' is only prospective, such an increase in power has the potential for abuse and the situations in which it might be authorised is vague and poorly particularised. ASIO, like any government agency, should not operate outside the scope of the law applicable to any other government agency and the very narrow circumstances that might justify such a power should not be framed in such broad terms.

[2] http://www bbc com/news/uk-27724805

Notwithstanding Blueprint's opposition to the introduction of SIOs, should they be introduced they should include the following additional protections–

a) improved oversight and approval for the obtaining of an SIO warrant,
b) further restriction on the types of conduct legitimised by an SIO,
c) restrictions on the length of an SIO with compulsory renewal periods,
d) the introduction of a 'special advocate' designed to represent the interests of the targeted person,
e) compensation for damage or loss suffered by innocent third parties as a result of any crime committed in connection with an SIO and
f) annual oversight by both houses of Parliament of the use and effectiveness of the amendments. These are detailed below:

(a) Improved approval and oversight for obtaining an SIO warrant

Under the Bill, an application for an SIO must be made to an 'authorising officer', which is defined as the Director-General, or a Deputy Director General. Considering the profound increase in power coupled with the profound decreasing in accountability that presents itself with the introduction of SIOs, the fact that such application only be made internally to the agency is an inappropriate concentration of power. In order for the grant of an SIO, approval should be sought from both an 'authorising officer' (whether that be the Director General or the Deputy Director General) and in addition both the Attorney General and the Federal Court of Australia (where the judge does not have a security clearance, such that a full separation from the intelligence community is achieved. This will ensure proper oversight of the grant of these warrants and it also ensures that the powers are more likely to be used wisely and in accordance with checks and balances currently existing at law.

Accordingly, proposed subsection (1) of section 35B of Schedule 3 should be re-drafted as follows:

"An ASIO employee must apply to:

(a) an authorising officer; and
(b) the Attorney General; and
(c) the Federal Court of Australia,

for an authority to conduct a special intelligence operation on behalf of the Organisation."

(b) Further restriction on conduct authorised by an SIO warrant

As SIO warrants represent a dramatic increase in powers, the following additional restrictions should be included in proposed section 35C of Schedule 3:

- Each SIO should be obtained by a warrant justifying the necessity of its status as an SIO, to be approved by each of an authorising officer, the Attorney General and a Judge of the Federal Court of Australia. Although proposed Section 35L of Schedule 3 states that an SIO does not allow for conduct not in accordance with a warrant, the SIO amplifies the power of a warrant because it changes the potential nature of the conduct. It therefore should be applied for in the same manner as the warrant itself;

- SIOs should only be applied for, and approved, where there is no other possible manner of obtaining the relevant intelligence from the target, this should have to be justified to the oversight authorities, and an SIO should always be proven as a last resort;
- Any perjury or contempt of court during the application, renewal, or any other matter before the Court cannot be excluded from liability by virtue of an SIO; and
- Any conduct occurring following the obtaining of an SIO warrant should only be authorised, and liability should only be limited where the conduct was in reasonable furtherance of that warrant. In other words, criminal conduct engaged in during the course of an SIO must be in furtherance of the warrant itself, the warrant does not excuse all criminal conduct.

The increase in the requirements to obtain an SIO are necessary to ensure that SIO's are just not labelled lightly or for convenience, in order to avoid proper oversight.

(c) Restrictions on the length of an SIO warrant and renewal periods

A further section should be included in the proposed section 35C to ensure that the period an SIO may be in force does not exceed 3 months. On the expiration of the 3-month period, ASIO must reapply for a renewal in the same manner proposed above (i.e. to the authorising officer, to the Attorney General, and to a judge of the Federal Court.

(d) Introduction of a 'special advocate'

Blueprint has long advocated for the inclusion of a special advocate to represent the interests of a potential target in the application for any kind of intelligence warrant. Currently, an advocate on behalf of ASIO appears before a closed session of court and argues the merits of that warrant. As the target is necessarily unaware of a surveillance warrant, they cannot appoint a lawyer to protect their interests. When making such an application, the lawyer for ASIO is under the normal ethical duty of a lawyer making an *ex parte* application to present both the case for the warrant and the case against it, when the potential powers on offer are so strong and so intrusive this is not enough. A lawyer independent both of the court and the intelligence community could be appointed to act on behalf of the target without the direct instruction of the target. Their duty would be to ensure that all proper argument is put to the judge in the application for the warrant.

In Blueprint's submission to this committee in respect of amendments to the *Telecommunications Act* on Wednesday 26 September 2012 during the provision of Blueprint's oral evidence to that committee:

> "*Mr Wolfe: I do not pretend to design the entire policy, but in simple terms it would be having trained advocates—lawyers who stand on the other side from ASIO's lawyers, if we use that as an example, to argue the case. Currently it works on an ex-parte basis. ASIO's lawyers ask for the warrant, of course subject to their legal professional obligations, which are to present the other side of the case. Having special advocates enables the other side of the case to be presented by somebody who is purportedly independent. I am not saying that the lawyers who currently request warrants on behalf of ASIO do not act within their full legal professional obligations, but it is also about the appearance of doing so. I think that the*

creation of special advocates only increases that appearance by having another independent step in the review of those warrants."[3]

(e) Compensation for innocent victims of crimes committed in connection with an SIO

If crimes are legitimised by the creation of SIOs then it follows that collateral damage and loss might be suffered as a result. At criminal law, compensation for victims of crime exists to protect those who have suffered directly or incidentally from the commission of a crime. In this case, as the crimes are state sanctioned, there is an increased onus on the Government to ensure that any innocent victim of the commission of a crime is properly compensated.

Accordingly, a provision should be included to the effect that any innocent victim of a crime that suffers personal, property or other damage should be compensated by ASIO to the full extent of the loss suffered.

(f) Annual reporting on the use and effectiveness of the amendments

A further clause should be included in the Bill as an amendment to the ASIO Act that provides that for each year, ASIO should publish a transparent and open report to the Attorney-General, and to the Parliament in respect of the following matters:

- The direct effect the Bill has had on the reduction of serious crime and terrorism;
- The number of times an SIO warrant was sought, was approved and the conditions placed on each warrant;
- The number of times an SIO warrant was extended, renewed or applied for in respect of the same intelligence operation (or an operation arising out of similar circumstances, targets or parties);
- A detailed description of each crime committed in connection with an SIO, the damage caused and a justification for the carrying out of that crime or damage;
- Detail of any crime committed in contravention of 35C(2)(e) of Schedule 3 (crimes not allowed even when subject to an SIO);
- Any compensation or rectification made in respect of any damage caused as a result of acting in an otherwise illegal capacity, which is legitimised by the warrant.

The above is a non-exhaustive list, and further reporting requirements may be added to this list. Importantly, the above requirements should be in addition to the already existing reporting requirements to which ASIO is subject. This report should be subject to questioning by any members of Parliament and their committees.

(g) Additional matters

The following additional matters should be rectified in the Bill:

- The word 'serious' should be deleted from proposed section 35C(2)(e) of Schedule 3. An SIO should not allow for injury of any kind, it is not enough to only forbid 'serious injury'.

[3] http://par nfo aph gov au/par Info/search/d sp ay/d sp ay w3p;db=COMMITTEES; d=comm ttees%2Fcomm nt%2F142792da-77a8-4e0e-b340-5fd973466c32%2F0004;query=Id%3A%22comm ttees%2Fcomm nt%2F142792da-77a8-4e0e-b340-5fd973466c32%2F0000%22

- Section 35C(3) of Schedule 3 should be amended to remove authorisation for 'unconditional' SIO authority. Any and all SIOs granted should be subject to the conditions set out in the warrant and on the terms added by the granting authorities (as proposed above, an authorising officer, the attorney general, and a Court.

Blueprint recommends that (a) SIOs should not be introduced, but if they are then (b) the provisions and definitions for such should be better particularised and transparent in the manner outlined in points (a) to (f) above.

4 Disclosure of Information in respect of 'Special Intelligence Operations'

The Bill, by its Schedule 3 and the insertion of a new Section 35P to the ASIO Act creates two new offences in respect of the disclosure of information about SIOs. An offence occurs if any person discloses information about an SIO, including an operative, a third party becoming aware of information about an operation and most chillingly, a journalist to whom another has disclosed. It carries a prison sentence of up to 5 years. The second offence relates to the same disclosure but increases the prison sentence up to 10 years where a person intend to endanger a person or interrupt intelligence operations, or the disclosure will danger a person or intelligence operation.

The EM by its paragraph 94 assures the committee that it would not otherwise limit the right of a whistleblower as such a person would still be able to make a disclosure in accordance with PIDA. However, as we argued in previous submissions to this parliament, the provisions relating to public interest disclosure in that Act are already very restrictive when revealing wrongdoing in the law enforcement and intelligence sector. Although it is naturally wise to keep some types of information secret for the purposes of protecting the national interest, intelligence agencies and the information attached to them should not be excluded simply by reason of this fact. Typically, in organisations where by design there is less publically available information, there is the greatest opportunity for wrongdoing.

Perhaps even more importantly, the extension of criminal conduct to a journalist by widening the definition to 'a person' will have a frightening effect on the ability of a journalist to publish stories in the public interest. The restriction on doing so presents a serious curtailment on the freedom of the press.

One does not need to look further than journalists such as Glenn Greenwald and Laura Poitras to see the value in protecting journalism as a method of promoting accountability in the intelligence and security sector. Without their work, along with other journalists' reports, we would not know about severe curtailment of our civil liberties.

One such example involved the Australian Defence Signals Directorate, through the 'five eyes' (Australia, the US, Canada, New Zealand and the United Kingdom) network ***boasted*** that it could ***provide unselected and unminimised metadata information on Australian citizens to other five eyes members without privacy constraints.*** Information might include legal, medical, religious and other personal material. http://www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens.

This is just one example of the public interest journalism reports that have emerged as a result of important disclosures, and indeed the journalistic integrity demonstrated in reporting them. It is clear that the purpose of this proposed legislation is to prevent reporting this type of governmental and

intelligence abuse and that if Greenwald and Poitras were subject to these provisions, they would be sent to prison. This is a situation to avoid at all costs. A strong democracy relies on a strong media to act as a mirror to governmental overreach and human rights abuses such as these where each Australian has been demonstrated to sacrifice their privacy for disproportionate government power. Further, the geographical extension proposed by proposed section 35P(4) and (5) means that foreign journalists are also prevented from reporting on this conduct. This sets a very bad precedent and will do significant damage to Australia's reputation as a democratic nation in the international community.

Moreover, the Bill would apply to information passed from a whistleblower to a member of parliament if that information was passed on outside of the immunities afforded by disclosure within the parliament. This, in effect, criminalises the representative functions of a member of parliament. In a hearing Blueprint provided both written evidence and oral evidence in December 2012 in respect of the *Public Interest Disclosure Act 2013*, a member of that committee Bronwyn Bishop MP recognised the importance of members of parliament assisting whistleblowers in the exposure of wrongdoing:

> "**Bronwyn Bishop MP**: *I do not think enough is made of the power of a member of parliament to represent and get justice for individuals. It is hugely powerful. Without disclosing a current case that I am dealing with, there is a real need for a remedy for a particular constituent that I have. As (a) member of parliament, I get access to people that an ordinary person cannot, and I really can put the case strongly and really can get outcomes. Far from trying to paint members of parliament, as is popularly done, as pariahs in some way, I think that the ability of members of parliament to represent and get justice for their people and to use the sort of reach that we have needs to be more broadly known."*

These provisions would criminalise an MP from receiving and discussing a disclosure made in respect of an SIO. If for example the information revealed a crime being committed and the MP needed to seek advice from an advisor, a lawyer, a fellow member of parliament or to engage in the public debate that would make the MP a criminal facing up to 10 years in prison - irrespective of the public interest nature of the disclosure. This is extremely worrying. It reflects a systematic attempt to gag any release of information in the public interest – whether by investigative journalists as outlined above, or by elected parliamentarians of our federal parliament.

Public interest disclosure, in all areas of government is a proven curtailment on corruption and abuse of power. This was acknowledged by the Commonwealth Government in 2012 when it passed the *Public Interest Disclosure Act 2013*. The criminalisation of journalism goes against this very important reform and it acts as a disincentive to those who come forward in the public interest to expose wrongdoing, corruption and abuse of power (as highlighted by the above).

In order to further this mechanism, Blueprint proposes that this section of the legislation must be deleted if Australia is to remain a country, which can lay claim to a free press and free speech.

In fact, not only should this section be deleted, but this set of amendments should be used to solidify the importance of public interest disclosure even in the intelligence community. One way to ensure this whilst striking a balance with maintaining the integrity of intelligence information is to introduce a public interest test to the proposed section 35P of the Schedule 3 to the Bill. This might be achieved by adding a sub-section 3(e) to the proposed section 35P of the Schedule 3 to the Bill, which would read as follows:

> *"Subsections (1) and (2) do not apply if the disclosure was…a public interest disclosure (as defined by the Public Interest Disclosure Act 2013 (Cth), unless (c) where the disclosure of the information to that person, or any person, could adversely affect a person's safety (other than an enemy combatant); or jeopardise the proper planning, execution, conduct or future conduct of a lawful defence, intelligence or law enforcement activity or operation, in such a way as may adversely affect a person's safety, whether directly or indirectly, including the safety of the general public."*

This proposed section reflects both an appreciation for the importance of disclosing information in the public interest, but also for the importance of maintaining the integrity of legitimate intelligence operations.

There is no other way to describe this amendment than to say that it criminalises journalism. Australia must not go down this path. Accordingly, proposed section 35P of the Schedule 3 to the Bill should be deleted. Not only should it be deleted, but the amendments should go further and protect those who come forward in the public interest to reveal wrongdoing, corruption and abuse of power.

5 Single Access warrant to a 'Network' of computers

Schedule 2 of the Bill, by the introduction of proposed sections 22 and 25A to the ASIO Act will broaden the definition of 'computer' to include all computers in a network. As explained in paragraph 5 of the EM:

> *"improving ASIO's intelligence collection powers by…enabling it to obtain intelligence from a number of computers (including a computer network) under a single computer access warrant, including computers at a specified location or those which are associated with a specified person".*

As we argued in our submission to the Legal and Constitutional Affairs Committee in February 2014 in respect of this matter and the PJCIS recommendation:

> *"The Committee recommends that the definition of computer in the Australian Security Intelligence Organisation Act 1979 be amended by adding to the existing definition the words "and includes multiple computers operating in a network".*
>
> *The Committee further recommends that the warrant provisions of the ASIO Act be amended by stipulating that a warrant authorising access to a computer may extend to all computers at a nominated location and all computers directly associated with a nominated person in relation to a security matter of interest."*[4]
>
> *This issue is similar to the issue with 'Recommendation 10', as an expansion of the definition of a 'computer' and an amendment to the warrant regime is not a problem in principle, so long as the access is proportionate to the alleged criminal conduct and the*

[4] PJCIS Report pp 89

> *effect on the privacy of the users and owners of a particular network of computers. It must be acknowledged that the more devices / systems accessed is an amplification of the invasion of privacy notwithstanding the fact that the reason those advocating for an extension of the definition of 'computer' are seeking to 'future proof' the legislation. By way of example, if the term 'computer' is extended to include a 'network of computers', on a plain reading of that definition it is easy to envisage a situation where a warrant to access a network of computers could have significant overreach. Here it is important to consider a context. Where the warrant seeks to access a personal network of computers, for example, a laptop, a tablet device and perhaps a desktop of a person operating off a personal wireless network run from that person's home, the potential for overreach is minimal. This reflects a sensible approach to the future proofing of the legislation. However, consider if the person allegedly engaging in criminal conduct is doing so from a workplace network, and that workplace is an international company with tens of thousands of computers on that same network. In that circumstance, the invasion of privacy extends to tens of thousands of irrelevant and unrelated machines / access points. Even in a smaller context, if the proposed extension applied to the computers belonging to other people living in a shared house, and those people are not or should not be under investigation, then accessing their computers is an unreasonable extension of powers. Physical proximity in the workplace or home to an individual who is being investigated should not of itself result in the violation of an ordinary Australian's computer equipment. Any amendment to the legislation must clearly express this limit on state powers.*
>
> *Therefore, if the definition of 'computer' is to be extended, a warrant should set out the extent of the network to which is applicable to the warrant. Further, a warrant to access a network should only be extended to the amount of computers on a network sufficient to investigate the wrongdoing, and directly controlled by the individual being investigated. This would achieve a reasonable balance between the future proofing of the legislation and insurance against the potential overreach of that amendment.*

The issue with the potential amplification of powers through the guise of streamlining and modernising legislation was in fact identified by Attorney-General George Brandis (then shadow Attorney-General when he stated in the PJCIS hearing on Wednesday 26 September 2012 during the provision of Blueprint's oral evidence to that committee:

> *"I suppose it is a bit like saying, 'Well, we have two or three security cameras in critical places in the city that survey crowd behaviour,' and saying, 'We are going to put a security camera on every street corner of Sydney.' It is not a different power but the range or the amplitude in which the existing power is exercisable really is so greater that it changes the character of it."*[5]

In this case, the extension of the definition of 'computer' has the danger to amplify the power to a significant extent and indeed create further potential for (at best) collateral damage and at worst,

[5] http://par_nfo aph gov au/par Info/search/d sp ay/d sp ay w3p;db=COMMITTEES; d=comm ttees%2Fcomm nt%2F142792da-77a8-4e0e-b340-5fd973466c32%2F0004;query=Id%3A%22comm ttees%2Fcomm nt%2F142792da-77a8-4e0e-b340-5fd973466c32%2F0000%22

abuse. Blueprint argues for the following definition of a computer to be replaced in proposed section 22 of the Schedule 2 to the Bill:

> *"computer means all or part of:*
>
> *(a) one or more computers; or*
> *(b) one or more computer systems; or*
> *(c) one or more computer networks; or*
> *(d) any combination of the above,*
>
> *where in any case the computer is controlled by the target, and each computer on a 'system' or 'network' is necessary to access for the purposes of investigating the target."*

The purpose of amending the section in this way is to ensure that entire networks of computers are not compromised in the investigation of a target. Consider an example where the target is an employee of a major corporate organisation working in the information technology department. Technically, they may have control over the entire network but the access should be limited only to the computers on that network necessary to the investigation. Blueprint understand the modernisation of this provision, but as it is currently drafted it present a major overreach to existing power not in line with the technological updating of the legislation.

Blueprint recommends that the definition of a computer be amended in the manner suggested above, which represents a future proofing of the legislation whilst still maintaining appropriate safeguards.

6 Amending the current limitation on the disruption of a computer

Schedule 2 of the Bill, by the amendment of sections 25(6) and 25A to the ASIO Act will remove the limitation of ASIO on its ability to "enable the use of a third party computer or communication 'in transit' for the purpose of accessing data on the target computer. As explained in paragraph 5 of the EM:

> *"improving ASIO's intelligence collection powers by… amending the current limitation on disruption of a target computer".*

As we argued in our submission to the Legal and Constitutional Affairs Committee in February 2014 in respect of this matter and the PJCIS recommendation:

> *"The Committee recommends that the Government give further consideration to amending the warrant provisions in the Australian Security Intelligence Organisation Act 1979 to enable the disruption of a target computer for the purposes of executing a computer access warrant but only to the extent of a demonstrated necessity. The Committee further recommends that the Government pay particular regard to the concerns raised by the Inspector-General of Intelligence and Security."*[6]
>
> *Blueprint believes that the disruption of a target computer (or network per Recommendation 20) is a very serious matter. Its seriousness is further amplified because the property of the*

[6] PJCIS Report pp 92

accused is violated in circumstances where the accused has not yet been charged with a crime.

Greater clarity is needed around this concept, such as the types of disruption necessary, details of the circumstances where there is a 'demonstrated necessity', and reassurance that whatever disruption was deemed necessary is fixed or rectified in some manner after it is no longer deemed necessary. The argument run by the law enforcement community seems to be 'sometimes we cannot exercise a warrant because a metaphorical door is closed. We need a hammer to break down that door so we can leave the metaphorical cameras inside'. What needs to be added to that discussion and argument is in what circumstances we let them break the door down, and making sure that they have fresh hinges and door sealant for when we deem that period is over. In addition, there must be explicit protections that the metaphorical camera is not being used to infringe the privacy of anyone other than the target of the investigation. Collateral damage to innocent Australians' data privacy is unacceptable. With so much of our modern life lived in an online setting, it crosses a dangerous line between legitimate investigation and Orwellian state-based surveillance of the citizenry.

Greater clarity is still needed on this concept and the protection included in proposed sub-section 25A(5) to not "materially" add, delete or interfere with a person lawfully using a computer gives little comfort. The fact that the provision extends to any computer (including third parties) in the exercise of an investigation amplifies the power and potentially adds to a curtailment of privacy and abuse.

As this is the case, particularisation of the ability to disrupt a computer is needed. The ability to do so should be restricted by the following factors:

- It should be demonstrated in the warrant obtained to disrupt the computer that this is the only manner in which the relevant intelligence can be sought from the target (disruption should be a last resort);
- In no circumstances should ASIO be able to disrupt a third party computer not directly associated with the target of an intelligence operation;
- Although it may be necessary to disrupt a machine to insert malware or otherwise to effect surveillance of that machine, in no way should the disruption be able to prevent the normal operation of that computer, nor should it prevent the target from being able to access data; and
- Any damage or loss suffered as a result of the disruption of a computer should be rectified or compensated from the relevant agencies' budget to the victim to the fullest extent of that loss or damage.

Blueprint strongly recommends that this provision be reconsidered and at least particularised in the manner set out above.

7 'Sunset clause' for the amendments proposed by the Bill

Each and every 2 years after these amendments are enacted, if enacted, a review should take place such that ASIO should have to justify the continued existence of these provisions. In order to

demonstrate this, they must refer to, and rely on the oversight reporting outlined above at paragraph 3 (f). The purpose of this is to ensure that the increase in powers for ASIO is not automatic, and there will be an evidence based manner to evaluate and analyse whether or not these increased powers have any actual effect on the prevention of serious crime or terrorism.

Accordingly, the following clause should be added to section 2 of the Bill (Commencement) as sub-section 3:

> *"All amendments passed by this Bill shall expire 2 years from the date of Royal Assent. ASIO must present a report to the parliament outlining the effectiveness of the legislation which shall be made publically available and the legislation may only be renewed if a Bill is introduced, reviewed, and passed by both house of parliament and community consultation has been sought through a committee process. Each time the provisions are re-enacted, they will be subject to the same 2 year re-evaluation process with the date of Royal Assent replaced as the date of the renewal of the amendments."*

8 Conclusion

Since this committee considered amendments to the *Telecommunications Interception Act* in 2012 and the subsequent committees that have dealt with increased powers to intelligence agencies, a fundamental shift has taken place in society that no longer tolerates the indiscriminate surveillance legitimised by such provisions. No less that 60 separate and shocking disclosures by Edward Snowden about the nature of **intelligence agencies having broken either laws or constitutional amendments and then having lied about it to the public and the legislative branch of government** have demonstrated the all-pervasive surveillance state that has begun to be built and in many cases already exists.[7] This is a surveillance state that has largely been hidden from public scrutiny. This Bill will increase powers that curtail freedoms and perversely, will criminalise both employees and journalists from revealing further abuse and wrongdoing. The approach does not reflect the current mood for transparency and distrust in what can only be described as the least transparent halls of government.

Blueprint would like to take the opportunity again to thank the committee for its time in considering our submission and reiterate its enthusiasm in assisting the committee further in whatever way it might deem us to be helpful.

Please contact us about this submission or any other matter.

Blueprint for Free Speech
6 August 2014

[7] Such wrongdo ng and es were revea ed recent y when the State Department n the US concurred w th the f nd ngs of the Senate Inte gence Comm ttee that not on y had the CIA engaged n torture s nce September 2011 but that they had ed to Congress above hav ng done so Perverse y the CIA has now adm tted to spy ng on member of the Senate Inte gence Comm ttee dur ng th s rev ew process http://www theguard an com/wor d/2014/ u /31/c a-adm ts-spy ng-senate-staffers