Committee Secretary
Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
Canberra ACT 2600
By email: legcon.sen@aph.gov.au

25 February 2014

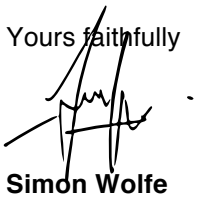
Dear sirs

Re: Submission to the Legal and Constitutional Affairs References Committee's (the Committee) Inquiry into comprehensive revision of the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIAA)

Please see **annexed** submission to the Committee, from Blueprint for Free Speech.

Please contact me should you have any queries in relation to this submission or any other matter.

Yours faithfully



Simon Wolfe
Head of Research
E: simon@blueprintforfreespeech.net

Blueprint For Free Speech
PO Box 187, Fitzroy VIC Australia 3065

Submission to the Legal and Constitutional Affairs References Committee's (the Committee) Inquiry into comprehensive revision of the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIAA)

25 February 2014

1 Introduction

Thank you for the opportunity to provide comments to the Committee in respect of its review of the TIAA.

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.

We are encouraged that the Federal Parliament wishes to consult with the community in respect of the wholesale changes proposed to the TIAA. Our primary concern, as always, is that the proposed changes do not negatively impact an individual's privacy or in any way undermine the sanctity of free communication between two or more people. This has the potential to occur where an overreach in state-sanctioned power may unduly undermine a citizen's privacy as they might feel reluctant to express a though or opinion for fear of their lack of privacy. This is very much at odds with the community standards of openness and freedom in Australia.

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 a supplementary submission providing information specifically on the efficacy of implementing a data retention regime (each a **PJCIS Submission**, together our **PJCIS Submissions**). Considering our involvement in the previous process, and as provided for in the scope of your request for consultation, our response to this Committee will focus on the (relevant) recommendations of the PJCIS Report.

Before we continue to the analysis of these recommendations, it is again disappointing to note that this discussion is taking place in an abstract sense. During the PJCIS inquiry, an almost universal criticism of the process was that the discussion paper was severely lacking in content and specific detail, especially on the most controversial of proposals. The community has again been asked to comment on the same themes, without a concrete draft of proposed legislation or other properly detailed description. One can only assume that further discussion will take place following the

release of a draft by the government, after this committee reports on the findings from the evidence it proposes to take. These series of inquiries have become a battle of attrition at great cost to the government and the interested groups wishing to contribute to this very important process. We are of course very honoured to be part of that process, but it should be kept in mind considering that we will likely have to have the same arguments again months or years down the track when something more tangible is proposed to the community.

The public mood regarding individual privacies is worthy of some study. Worth noting are two very recent polls. The first, published in February 2014, shows that Australians are increasingly concerned about their privacy compared to five years ago, particularly their online privacy.[1] The second, published in January 2014, shows a drop in trust levels of government internationally.[2] While the surveys were conducted separately, taken together they suggest a desire among the broader population for government to consider better controls of, and perhaps a drawing back of, state-based powers which it may use to infringe the privacy of the individual citizen.

2 PJCIS Recommendations

As stated above, the logical starting point is to discuss the recommendations provided in the PJCIS Report. We wish to focus on the recommendations we consider to be the most important for the re-shaping of telecommunications legislation.

(a) Recommendation 5

"The Committee recommends that the Attorney-General's Department review the threshold for access to telecommunications data. This review should focus on reducing the number of agencies able to access telecommunications data by using gravity of conduct which may be investigated utilising telecommunications data as the threshold on which access is allowed."[3]

Blueprint strongly agrees with Recommendation 5 – that the threshold for access to telecommunications data should be heightened. This of course rests on the principle that not only is it the manner and scope of the access, but also the frequency and ease of same. As George Brandis MP (now Attorney-General) stated in the PJCIS hearing on Wednesday 26 September 2012 during the provision of Blueprint's 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*

[1] Germano, J. 'Symantec survey reveals Australians concern about online privacy,' WhaTech, 17 Feb, 2014. See: http://www.whatech.com/members-news/security/18570-symantec-survey-reveals-australians-concerned-about-online-privacy

[2] Edleman, 'Trust in Government Plunges to Historic Low,' Edelman Trust Barometer. 19 Jan, 2014. See: http://www.edelman.com/news/trust-in-government-plunges-to-historic-low/

[3] PJCIS Report pp 26

amplitude in which the existing power is exercisable really is so greater that it changes the character of it."[4]

The point here is that the less cameras – or in this case – the fewer number of agencies with access to telecommunications data, the less potential there is for the abuse of such access. It is not the type of access that changes, but rather those who might have the privilege.

Blueprint believes that there must be proper public consultation about the detail around which agencies should have continued access to telecommunications data, and threshold proper description of the basis for this access and the threshold for same. This information should not be concealed from the broader Australian community, and Australians must have a say in this decision process. These details are critical in the execution of this in order, and to properly protect Australians' privacy rights.

(b) Recommendation 6

"The Committee recommends that the Attorney-General's Department examine the standardisation of thresholds for accessing the content of communications. The standardisation should consider the:

- *privacy impact of the threshold;*
- *proportionality of the investigative need and the privacy intrusion;*
- *gravity of the conduct to be investigated by these investigative means;*
- *scope of the offences included and excluded by a particular threshold; and*
- *impact on law enforcement agencies' investigative capabilities, including those accessing stored communications when investigating pecuniary penalty offences."* [5]

Blueprint does not oppose the standardisation of warrants save for the fact that the new 'standard' must not be lowered to the current lowest common denominator. Relevantly, the administrative benefit of streamlining the warrant process should not be used in a way to lower the threshold for an agency's ability to apply for a warrant.

Blueprint agrees with the PJCIS Committee's suggestions on the types of items that must be included in the application for a warrant. It is important to measure the proportionality of the suspected offence and any possible probative evidence purported to be gathered against the potential damage to privacy of the individual who owns the information or possesses/controls the potential evidence.

Specifically, the focus on the proportionality of the offence to the level of privacy intrusion is very important considering some of the dangerous arguments being made in favour of increasing the

[4] http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;db=COMMITTEES;id=committees%2Fcommjnt%2F142792da-77a8-4e0e-b340-5fd973466c32%2F0004;query=Id%3A%22committees%2Fcommjnt%2F142792da-77a8-4e0e-b340-5fd973466c32%2F0000%22

[5] PJCIS Report pp 30

ability to obtain an interception warrant for non-serious criminal offences. Consider the following made by the Western Australian Police in its submission to the PJCIS (and extracted by the Committee in its report):

> *"At present, under the TIA Act, it is not possible to obtain an interception warrant with respect to offences which carry a penalty of less than 7 years imprisonment but which may be preparatory to more serious offending. For example, precursor or preparatory crimes could include selling unregistered firearms, pervert the course of justice or stealing a motor vehicle. The ability to intercept communications in relation to precursor offences may assist in the prevention of more serious offending."*[6]

This argument is incredibly worrying. It focuses on the assumption that where one particular crime is committed, then because the likelihood (not evidence, not reasonable suspicion) of the committing of a further offence supposedly increases, this warrants and justifies the surveillance of the non-serious offence. An equally rational argument would include monitoring the telephone activity of a seven-year-old girl after she has stolen a chocolate bar from the supermarket as such behaviour increases the likelihood of serious financial embezzlement in her later adult life.

The Law Council of Australia, in its submission to the PJCIS[7], has developed a sounder approach in consistency and reasonableness in the application for a telecommunications interception warrant and stored communication warrants. The important element is to consider raising the bar for all such interception warrants applying only to 'serious criminal offences' and for there to be a robust and clear definition of what constitutes a 'serious criminal offence'. It certainly should not include so-called 'pre-cursor' offences. This makes sense from both an administrative point of view, in the sense that it erodes inconsistency in the warrant application process, but it also makes sense because the level of privacy intrusion does not change because of the method of the intrusion. If the access to communications is taken either before, during or after the communication was made it does not change the nature of the intrusion. It must be demonstrated that the access was made proportionate to the conduct and the only reasonable threshold for this must be 'serious criminal offences'.

(c) Recommendation 10

"The Committee recommends that the telecommunications interception warrant provisions in the Telecommunications (Interception and Access) Act 1979 be revised to develop a single interception warrant regime.

The Committee recommends the single warrant regime include the following features:

- *a single threshold for law enforcement agencies to access communications based on serious criminal offences;*

[6] PJCIS Report pp 27
[7] PJCIS Report pp 28

- *removal of the concept of stored communications to provide uniform protection to the content of communications; and*
- *maintenance of the existing ability to apply for telephone applications for warrants, emergency warrants and ability to enter premises.*

The Committee further recommends that the single warrant regime be subject to the following safeguards and accountability measures:

- *interception is only authorised when an issuing authority is satisfied the facts and grounds indicate that interception is proportionate to the offence or national security threat being investigated;*
- *rigorous oversight of interception by the ombudsmen and Inspector-General of Intelligence and Security;*
- *reporting by the law enforcement and security agencies to their respective Ministers on the effectiveness of interception; and*
- *Parliamentary oversight of the use of interception."*[8]

In theory, there should be no issue with a single interception warrant regime, so long as it is proportionate to the wrongdoing is accompanied by an acknowledgement that the more devices / systems accessed is an amplification of the invasion of privacy from accessing one device. This is the same argument referred to above per Recommendation 5 – that where the power itself is not being changed (i.e. the demonstration of the need to be granted a warrant to investigate a particular offence) but rather the scope to which that power can be applied changes the nature of the power itself. In other words, where a single interception warrant applies to twenty devices instead of one, the nature of the power can be changed by virtue of its amplification.

In Blueprint's written submission to the PJCIS, we advocated for the introduction of 'special advocates' to act on behalf of the person(s) to which a warrant for interception applies. In cases where the law enforcement agency believe the matters too sensitive or secret, the special advocate would represent the interests of the client, without actually notifying or meeting the client itself. As Blueprint argued in oral submission, in the context of ASIO seeking a warrant:

> *"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*

[8] PJCIS Report pp 48

creation of special advocates only increases that appearance by having another independent step in the review of those warrants."[9]

When updating and modernising the process of obtaining a warrant, it would seem prudent that both sides of the coin – those who are applying and those who are resisting – are given adequate and fair tools in that new streamlined process.

(d) Recommendation 13

"The Committee recommends that the Telecommunications (Interception and Access) Act 1979 be amended to include provisions which clearly express the scope of the obligations which require telecommunications providers to provide assistance to law enforcement and national security agencies regarding telecommunications interception and access to telecommunications data."[10]

Clear obligations for telecommunications companies are important as it apportions responsibility and transparency properly between the government and the private sector. It forces a company to be open about when, why, how and what is shared with government and allows a customer to understand their rights, especially with respect to the privacy of their data.

It is bad policy to expect the private sector to perform the role of government, especially when it comes to the gathering of evidence for serious criminal conduct. It is extremely bad policy if the private sector is unaware of its responsibilities, or the community in general is unaware of the obligations of their telecommunications providers with respect to the data given to them.

What is of primary importance is that the private sector should not be performing the government's policing duties, and the community as well as the companies themselves should be assured that this is not their role.

(e) Recommendation 16

"The Committee recommends that, should the Government decide to develop an offence for failure to assist in decrypting communications, the offence be developed in consultation with the telecommunications industry, the Department of Broadband Communications and the Digital Economy, and the Australian Communications and Media Authority. It is important that any such offence be expressed with sufficient specificity so that telecommunications providers are left with a clear understanding of their obligations."

An offence where a person does not provide assistance with the decryption of a document is dangerous for several reasons, detailed as following –

[9] http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;db=COMMITTEES;id=committees%2Fcommjnt%2F142792da-77a8-4e0e-b340-5fd973466c32%2F0004;query=Id%3A%22committees%2Fcommjnt%2F142792da-77a8-4e0e-b340-5fd973466c32%2F0000%22

[10] PJCIS Report pp 54

i. It is an entirely different matter to require a telecommunications provider to provide assistance with the decryption of material, and of that which might apply to a private individual. The reason for this is that the information to which the encrypted material usually pertains is of a private nature. In order to maintain the privacy of a document or data, the individual must maintain, (importantly, not waive) this privacy. For example, an individual might waive their right to encryption of particular data in a telecommunications agreement with their provider and any data not personally encrypted (by the individual rather than the provider), might have waived its privacy to the extent that the individual has granted this to the provider. To use an example, an email sent from the individual to another party not encrypted at their personal level cannot reasonably be expected to have the same level of privacy as one that has. Implicitly, they have ceded some privacy over its content to the telecommunications provider. However, if they have exercised that right to privacy by personally encrypting the email, they have exercised this right to privacy and therefore it should be more difficult to force that individual to decrypt.

ii. If power is granted to a law enforcement body to force an individual to decrypt a communication they have encrypted, this will have a considerable implication on an individual's right to silence, and their privilege against self-incrimination. Where the interception being made is in furtherance of the prosecution of that individual for criminal conduct, it would be inappropriate (and certainly counter to the intention of hundreds of years of common law and existing Federal and State legislation) for that individual to assist the prosecution in their case against them.

iii. Apart from the theoretical legal argument, there are many practical considerations to account for, such as forgotten passwords, denial of encryption or denial of knowledge of the encryption. If the individual claims that they're neither are aware of the encryption, or cannot practically assist with the decryption for some other legitimate reason, it would be unfair that such an individual would be punished for failing to assist. This is certainly the case if they are answering honestly, but even if they are not answering honestly, how can reasonable legislation be built to prove otherwise? It would seem difficult to prove that a person is not assisting with decryption if they insist on one of the legitimate excuses above, especially considering the prevailing assumption of innocence.

iv. To force an individual to assist with the decryption of data could have serious implications on other legitimate privileges asserted by individuals. Once the data is decrypted, the privilege is lost. Consider for example:
    - The implication on shield laws where a journalist wishes to protect the integrity or physical safety of a source;
    - Legal professional privilege;
    - Private medical records; and
    - Many other instances of legitimate privilege.

There is a danger than in an attempt to 'future proof' legislation and criminal investigations that in doing so it can damage the important legal and democratic history built over hundreds of years. The future proofing of these investigative methods should not come at the cost of the seminal building blocks of democracy including innocence until proof of guilt, the right to silence, the privilege against

self incrimination and the secrecy between an individual and their lawyer, their doctor, their journalist.

For these reasons, Blueprint opposes the development of such an offence.

(f) Recommendation 20

"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."[11]

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 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

[11] PJCIS Report pp 89

between the future proofing of the legislation and insurance against the potential overreach of that amendment.

(g) Recommendation 21

"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."[12]

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 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.

(h) Recommendation 22

"The Committee recommends that the Government amend the warrant provisions of the Australian Security Intelligence Organisation Act 1979 to allow ASIO to access third party computers and communications in transit to access a target computer under a computer access warrant, subject to appropriate safeguards and accountability mechanisms, and consistent with existing provisions under the Telecommunications (Interception and Access) Act 1979."[13]

Blueprint repeats its concerns made in relation to Recommendation 21, however, says further that where a third party computer is used for the purpose of targeting a primary computer, the three elements of legitimacy, necessity and proportionality must be fulfilled.

[12] PJCIS Report pp 92
[13] PJCIS Report pp 95

In reality, the view of the Office of the Victorian Privacy Commissioner should be 'front of mind'.[14] Essentially, any such mechanisms including the ability to disrupt a target computer per Recommendation 21 or the ability to use a third party computer to target a primary computer should be a last resort. Any effort to use these means by an agency should reflect this fact. It is a sobering thought to consider that these are the sorts of powers "*usually characteristic of a police state*".[15]

(i) Recommendations 42 and 43 – Data Retention Scheme

Recommendation 42 –

"There is a diversity of views within the Committee as to whether there should be a mandatory data retention regime. This is ultimately a decision for Government. If the Government is persuaded that a mandatory data retention regime should proceed, the Committee recommends that the Government publish an exposure draft of any legislation and refer it to the Parliamentary Joint Committee on Intelligence and Security for examination. Any draft legislation should include the following features:

- *any mandatory data retention regime should apply only to meta-data and exclude content;*
- *the controls on access to communications data remain the same as under the current regime;*
- *internet browsing data should be explicitly excluded;*
- *where information includes content that cannot be separated from data, the information should be treated as content and therefore a warrant would be required for lawful access;*
- *the data should be stored securely by making encryption mandatory;*
- *save for existing provisions enabling agencies to retain data for a longer period of time, data retained under a new regime should be for no more than two years;*
- *the costs incurred by providers should be reimbursed by the Government;*
- *a robust, mandatory data breach notification scheme;*
- *an independent audit function be established within an appropriate agency to ensure that communications content is not stored by telecommunications service providers; and*
- *oversight of agencies' access to telecommunications data by the ombudsmen and the Inspector-General of Intelligence and Security."*[16]

Recommendation 43 –

"The Committee recommends that, if the Government is persuaded that a mandatory data retention regime should proceed:

- *there should be a mechanism for oversight of the scheme by the Parliamentary Joint Committee on Intelligence and Security;*
- *there should be an annual report on the operation of this scheme presented to Parliament; and*

[14] PJCIS Report pp 93
[15] PJCIS Report pp 93
[16] PJCIS Report pp 192

- *the effectiveness of the regime be reviewed by the Parliamentary Joint Committee on Intelligence and Security three years after its commencement."*[17]

As the Committee highlights in the PJCIS Report, the majority of the evidence taken during the inquiry concerned the inclusion of a data retention scheme in the TIAA. One of the hurdle issues for the committee during that inquiry, and indeed for those seeking to make comment on the proposal, was the dearth of information in the proposal. In the original discussion paper, two lines were provided on what was easily considered to be the most contentious topic. Similarly here, although we have the benefit of the PJCIS's analysis of the evidence both for and against the abstract notion of a data retention scheme, we still do not have draft legislation on which to comment or suggest for amendment. This, again, is a significant hurdle.

As the Committee noted, Blueprint provided a substantial submission to the PJCIS on the issues raised in the discussion paper as well as a substantial volume of documents on the efficacy of data retention, primarily in the European context (on which it is assumed such a scheme in Australia will be built). We continue to rely on the points made in those submissions. We again stress that **we are strongly against the introduction of a data retention regime**.

However, in the context of the government potentially considering the implementation of such a regime, we make the following comments in respect of that highly undesirable outcome:

- Whilst data retention should apply only to metadata, and not to the content of documents, the term 'metadata' needs careful definition. As was noted during the oral submissions of the PJCIS hearings, often the metadata can reveal the nature, persons or substantial content of a communication.
- We are especially encouraged by the committee recommending that in circumstances where the metadata cannot be separated from the content, the metadata should be treated as content. Further, the exclusion of Internet browsing data is very positive.
- The storage of any data collected as part of a data retention regime should be done securely, and it should be stored on Australian soil, and administered by the Australian Government. Should the information be held or controlled by a company of a foreign power, it would pose a real and serious risk to the sovereignty of Australia.

Additionally, Blueprint is highly encouraged by the other caveats created in Recommendations 42 and 43. These recommendations are reflective of the potential danger that such a regime will create. The safest way to prevent danger arising, of course, is not to enact a data protection regime at all. Failing that, the recommendations above provide a starting point to at least allow some protection.

It should be noted that since Blueprint last provided its written and oral submissions, the Advocate General of the Court of Justice of the European Union has issued an opinion on the European

[17] PJCIS Report pp 193

Directive requiring the data retention regime (Directive 2006/24/EC). In its media release, it summarised the Advocate General's opinion:

> *"The Advocate General points out, in this regard, that the use of those data* [ed. metadata] *may make it possible to create a both faithful and exhaustive map of a large portion of a person's conduct strictly forming part of his private life, or even a complete and accurate picture of his private identity. There is, moreover, an increased risk that the retained data might be used for unlawful purposes which are potentially detrimental to privacy or, more broadly, fraudulent or even malicious. Indeed, the data are not retained by the public authorities, or even under their direct control, but by the providers of electronic communications services themselves. Nor does the Directive provide that the data must be retained in the territory of a Member State. They can therefore be accumulated at indeterminate locations in cyberspace."* [18]

3 Introduction of a 'proportionality test'

A common theme throughout each of the recommendations above, and our responses to them, is that there is a strong need to constantly balance the proportionality of the invasion of privacy with the necessity of the investigation and the methods used. In the application for any interception warrant, a statement should be required by the party seeking that warrant, which sets out an explanation of how the commensurate invasion of privacy is proportionate to the investigation method proposed to be used. In other words, a detailing of the particulars of the privacy proposed to be invaded and an explanation of why it is necessary to undermine that right to privacy by pursuing an interception.

Whilst this issue has been touched on elsewhere in this submission, Blueprint recommends that the principles set out in the seminal case of *Weber and Saravia v Germany*[19], which set out the following minimum safeguards for when an interception warrant should be granted and for which Blueprint urges to be implemented as legislation. These principles are:

- the nature of the offences which may give rise to an interception order;
- a definition of the categories of people liable to have their telephones tapped;
- a limit on the duration of telephone tapping;
- the procedure to be followed for examining, using and storing the data obtained;
- the precautions to be taken when communicating the data to other parties; and
- the circumstances in which recordings may or must be erased or the tapes destroyed.[20]

[18] http://malte-spitz.de/wp-content/uploads/2013/12/CP130157EN.pdf, the full decision may be found at http://curia.europa.eu/juris/documents.jsf?num=C-293/12

[19] Application no. 54934/00 by Gabriele WEBER and Cesar Richard SARAVIA against Germany, The European Court of Human Rights (Third Section), sitting on 29 June 2006

[20] For a copy of the full decision, see http://echr.ketse.com/doc/54934.00-en-20060629/view/

Further, consideration should be given to the "Guidelines of the Committee of Ministers of the Council of Europe on human rights and the fight against terrorism" from 2002[21], which provide further privacy protection to ensure that a proportionate measure is more easily taken:

> *"COLLECTION AND PROCESSING OF PERSONAL DATA BY ANY COMPETENT AUTHORITY IN*
> *THE FIELD OF STATE SECURITY*
> *Within the context of the fight against terrorism, the collection and the processing of personal data by any competent authority in the field of State security may interfere with the respect for private life only if such collection and processing, in particular:*
> *(i) are governed by appropriate provisions of domestic law;*
> *(ii) are proportionate to the aim for which the collection and the processing were foreseen;*
> *(iii) may be subject to supervision by an external independent authority.*
>
> *MEASURES WHICH INTERFERE WITH PRIVACY*
> *Measures used in the fight against terrorism that interfere with privacy (in particular body searches, house searches, bugging, telephone tapping, surveillance of correspondence and use of undercover agents) must be provided for by law. It must be possible to challenge the lawfulness of these measures before a court."*[22]

The Committee spoke often and at length about achieving a balance between the rights of citizens to their own privacy and the need of law enforcement agencies to be able to protect Australians from threats and danger to national security. However, this was mostly discussed in a policy making context – in the design and balance of legislation. Blueprint understands that this balance needs to be achieved, however there is no reason why such a question might not be asked by the person applying for a warrant on each occasion one is sought or why it should not be considered in the normal course of duty of those charged with such powers

The idea of creating a 'proportionality test' means that this balancing act is made every time someone's privacy is to be invaded, or is kept 'front of mind' for those with power to undermine privacy, not only every time the legislation is sought to be amended. It would be a strong step in the right direction not only to provide some clarity around the warrant application process and the general obligations of law enforcement officers but also so that all parties will be informed of the consequences of interception.

Accordingly, Blueprint strongly recommends that:

(a) a 'proportionality test' be added to the warrant provisions of the legislation such that every time a warrant is sought, a justification of the proportionality of such conduct is provided; and
(b) a general obligation be included in the legislation which requires a person in the normal course of their duties, including when acting within the powers granted by a warrant, to consider the on-going proportionality of their actions to the invasion of privacy.

[21] https://wcd.coe.int/ViewDoc.jsp?id=991179
[22] https://wcd.coe.int/ViewDoc.jsp?id=991179

4 Conclusion

The 21st century poses problems for law enforcement in a way not previously experienced. The issue at the heart of the debate is that those enforcing the law and those seeking to evade the law are now empowered with equally powerful tools. This is the new reality.

However, it is counterintuitive to redress this new balance by taking away fundamental freedoms built over hundreds of years. It is counterintuitive because in the manner proposed it has not only proven to be ineffective, but it eradicates the democratic values we are all trying to protect.

It is prudent to modernise the legislation to account for new technology and new challenges faced in gathering evidence for criminal investigations. It would be unreasonable for anyone to suggest otherwise. However, it is the duty of each of us to be vigilant against an overreach in the power of the state over its citizens.

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
25 February 2014