



AUSTRALIAN
LAWYERS
FOR
HUMAN RIGHTS

22 August 2014

PO Box A147
Sydney South
NSW 1235
DX 585 Sydney

alhr@alhr.asn.au
www.alhr.asn.au

The Committee Secretary
House of Representatives Standing Committee on Infrastructure and Communications
PO Box 6021
Parliament House
Canberra
ACT 2600

Dear Secretary

Australian Lawyers for Human Rights (ALHR) is pleased to provide this submission in relation to section 313 of the Telecommunications Act 1997 (the Act).

ALHR's primary concern is that the Act and section 313 should adhere to international human rights law and standards. We endorse the '*International Principles on the Application of Human Rights to Communications Surveillance*' (**International Principles**) in this regard.

Section 313 has a very wide ambit by virtue of section 313(7) and we submit that section 313 should be amended to meet a standard of clarity and precision that is sufficient to ensure that it can be applied transparently, subject to judicial review, in accordance with the Westminster system which is fundamental to Australia's constitutional democracy. Without such clarifications, the section places an inappropriate burden on communications providers as well as arguably breaching accepted international human rights and civil liberties in relation to online communication and privacy.

The Committee is considering only the issue of "government agency use of section 313 for the purpose of disrupting illegal online services" (neither 'disrupting' nor 'illegal online services' are defined). References in this submission to section 313 should be read as references to the use of section 313 for that purpose.

1.	Summary of Responses	2
2.	Clarifications	2
2.1	What 'requests' are referred to?	2
2.2	What does 'disruption' mean?	2
2.3	What are illegal online services?	3
2.4	What are 'potential' illegal online services?	3
3.	The Problems	4
3.1	Drafting precedes the widespread use of the internet	4
3.2	Practical problems and unforeseen consequences	4
3.3	Negative Impact upon human rights	5
4.	Transparency and Accountability	5
4.1	Background	5
4.2	Changes in transparency under Australian legislation	6
4.3	Transparency, accountability and section 313	7
5.	Modern practices in other countries	8
6.	Terms of Reference Questions	10
	Does section 313 meet the International Principles on the Application of Human Rights to Communications Surveillance?	14

1. Summary of Responses

- (1) No government agency or officer should be permitted to disrupt online services on the basis that they are 'potentially' in breach of Australian law. This is an overbroad interpretation of the current law and shows clearly that the section is not appropriately limited to those means which are strictly and demonstrably necessary to achieve a legitimate legislative aim with the minimum impact upon human rights.
- (2) Only services established to be involved in serious crimes or that directly incite serious crimes should be covered by the section.
- (3) It should be established before an Australian court or tribunal that a service is in breach of Australian law before any further action can be taken. Agencies should be authorised by a 'blocking' warrant issued by a court or tribunal which is subject to the tests of necessity and proportionality in order to make a 'request' for assistance to a carrier.
- (4) The agencies should be limited to law enforcement agencies.
- (5) Section 313 should be amended to include transparency and accountability measures including:
 - (a) necessity for 'blocking' warrant and related tests;
 - (b) appointment of special advocates to act on behalf of persons to whom a blocking warrant applies¹ and/or Public Interest Monitor
 - (c) compensation to be paid for any disruption to legitimate businesses who are incorrectly blocked in error (eg because they share the same shared web hosting space);
- (6) There should also be oversight of such requests by a Parliamentary Joint Committee, and an annual report on such requests presented to Parliament² including:
 - (a) number of requests;
 - (b) basis for requests;
 - (c) costs to the Government and costs to ISPs of implementing and managing the implementation of blocks;
 - (d) policies followed by government agencies in making such requests;
 - (e) outcome of requests – whether any legitimate sites were incorrectly blocked;

Judicially reviewed legislation is the key to transparency and accountability. If one accepts our existing Westminster system of democratic Australian government, then effectively one must agree that we should only be regulated by 'law,' and anything not able to be scrutinised by the judiciary is not 'law'.

2. Clarifications

2.1 What 'requests' are referred to?

Section 313 does not use the term 'requests'. The Terms of Reference state that 'How law enforcement agencies use section 313 to request the disruption of such services is an important public policy question.' Presumably the reference to 'requests' in the TOR is intended to refer to the process under section 313 whereby a Commonwealth, State or Territory officer or authority requires assistance from a carrier, carriage service provider, or carriage service intermediary ('carrier request'), rather than a process whereby government officers or agencies seek authorisation (for example, a warrant from a court or tribunal) to require that carrier assistance ('authorisation request'), given that the Act does not provide for authorisation requests. This interpretation is confirmed by the fact that the template used by the Australian Federal Police in communicating with ISPs pursuant to section 313 is phrased as a 'request for assistance.'

2.2 What does 'disruption' mean?

While the terms of reference refer to the AFP Access Limitation Scheme (to reduce the online availability of child abuse material³) which relies on providing service providers with an Interpol list of websites to be blocked at

¹ Blueprint for Free Speech, Submission to the Legal and Constitutional Affairs References Committee's Inquiry into comprehensive revision of the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA), 25 February 2014, p 6, <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Comprehensive_revision_of_TIA_Act/Submissions>, accessed 18 August 2014

² Compare with Administrative Appeals Tribunal Annual Report 2012-2013 <<http://www.aat.gov.au/Publications/AnnualReport/AnnualReport2013.htm>> accessed 18 August 2014.

³ FOI Documents released to Delimiter by Australian Federal Police <<http://delimiter.com.au/docs/Final-documents.pdf>> discussed in Renai LeMay, 'Redacted: AFP cuts ISP details from filter docs', *Delimiter* (27 February 2013)

Domain Name System (DNS) server level, the use of section 313 to ‘disrupt’ online services can involve other types of filtering or blocking⁴. The two major technical approaches are Technical Blocking and search result Removals.⁵

Blocking: common methods used to block access to specific Web Pages, domains, or IP addresses where direct jurisdiction or control over websites are beyond the reach of authorities involve:

- Internet Protocol (IP) Blocking blocks the addresses of a server. Web hosting providers generally host several (thousand) websites on one server;
- DNS tampering involves blocking one website (which may however have sub-websites eg blogging platforms);
- Uniform Resource Locators (URL) blocking using a proxy allows the filter to target specific items on a specific domain;
- Keyword/image blocking, which blocks access to websites based on the words found in URLs or blocks searches involving blacklisted terms or images.

Removals: companies that provide Internet search services cooperate with governments to omit illegal or undesirable websites from search results, making finding the sites more difficult.⁶

2.3 What are illegal online services?

“Illegal online services” are not defined in the Act and the issue of whether content provided by a particular website is illegal or not can be a vexed one. In Europe, there have been calls for clearer European-wide definitions.⁷ We note that Australia and New Zealand apparently have different views as to what content is regarded as ‘offensive’ – and therefore potentially illegal.⁸

Apparently web content that is hosted in Australia may be subject to a takedown request from the Australian Communications and Media Authority (ACMA) if the Office of Film and Literature Classification finds that it falls within certain categories as defined by the Commonwealth Classification (Publications, Films and Computer Games) Act 1995. The classification system chosen for Internet content is the more restrictive standard used for films, rather than the publications classification.⁹ As a result, some content which would not be regarded as illegal ‘offline’ is regarded as illegal when it is online.¹⁰

Conversely, material which is illegal – for example under section 18C of the Racial Discrimination Act – is not necessarily assessed.

Different States and Territories in Australia have instituted various laws that criminalize the downloading of illegal content and the distribution of content that is “objectionable” or “unsuitable for minors.” However their laws are not always consistent. It is unclear if the reference to ‘online illegal services’ is intended to capture material that is illegal under State or Territory legislation.¹¹

2.4 What are ‘potential’ illegal online services?

This term is not used in the section and would appear to reflect an unreasonably broad interpretation of the concept of preventing a communications service from being involved in committing an offence, which dangerously widens the scope of the legislation. The emphasis appears to be rather on the concept of

⁴ <<http://delimiter.com.au/2013/02/27/redacted-afp-cuts-isp-details-from-filter-docs/>> accessed 18 August 2014.

⁵ Peter A. Craddock, “Legal Implications of Internet Filtering” <<http://www.arpia.be/public/PACraddock%20-%20Legal%20Implications%20of%20Internet%20Filtering.pdf>> p 3.

⁶ OpenNet Initiative, “About Filtering” <<https://opennet.net/about-filtering>> accessed 8 August 2014.

⁷ ibid

⁸ Pinsent Masons Lawyers, “Data protection watchdog calls for single definition of ‘illegal content’ across EU”, 18 Sep 2012, <<http://www.out-law.com/articles/2012/september/data-protection-watchdog-calls-for-single-definition-of-illegal-content-across-eu/>> accessed 8 August 2014.

⁹ OpenNet Initiative, “Australia and New Zealand” <<https://opennet.net/research/regions/australia-and-new-zealand>> accessed 8 August 2014

¹⁰ Thus in 2008 and for some time thereafter the Australian Government proposed to require all ISPs in Australia to use ISP-level filtering to block overseas hosted - Refused Classification (RC) material on ACMA’s RC Content list: Craddock, op cit, p 8, <http://www.nytimes.com/2008/12/12/technology/internet/12cyber.html?_r=2&> accessed 15 August 2014.

¹¹ OpenNet Initiative, “Australia and New Zealand”, op cit, in relation to footnote 10 on that page, and see ALRC Report 118 Classification – Content Regulation and Convergent Media, ALRC 2012 [Executive Summary] <<http://www.alrc.gov.au/publications/executive-summary/background-1>>

¹² See OpenNet Initiative, “Australia and New Zealand”, op cit, in relation to the text relating to footnote 15 and following on that page, accessed 8 August 2014

preventing the offence from being committed in the first place – that is, involving the carrier in attempting to prevent a ‘potential’ offence from arising - rather than shutting down an existing serious offence.

In the UK, a legal test must be met as to whether content is illegal before a hosting site can be requested to remove that material¹². Impinging upon a person’s rights on the basis of “potential” illegality is inherently likely to be a “[risk] to democracy and to the freedoms of citizens.”¹³

The apparent intention of using section 313 to block services that are ‘potentially’ illegal demonstrates clearly that the section is not appropriately limited to those means which are strictly and demonstrably necessary to achieve a legitimate legislative aim with the minimum impact upon human rights.

3. The Problems

3.1 Drafting precedes the widespread use of the internet

Section 313 was drafted at a time when minimal information could be accessed through communications technologies and therefore its drafting did not take into account:

- the modern and changing technologies and techniques of the State, the ability of the State to combine and organize information gained from different surveillance technologies and techniques, or the increased sensitivity of personal information available to be accessed;
- the necessity for transparency and accountability in this area (see section 4)
- the way in which modern technologies could impact upon human rights (see 3.3);
- practical problems in utilising the section (see 3.2);
- modern practices in other countries (see section 5).

3.2 Practical problems and unforeseen consequences

Requiring the removal of illegal content at source is more effective than ‘disruption’¹⁴ but not necessarily possible outside Australia’s jurisdiction. Blocking therefore tends to be used by Australian agencies against sites which are outside Australian jurisdiction.

However when used against Australian sites, blocking has resulted in the disruption of thousands of legitimate sites with completely legal content, to the commercial disadvantage and inconvenience of the owners. It seems that this is a consequence which should have been foreseen. OpenNet Initiative says¹⁵ that:

Many blacklists are generated through a combination of manually designated web sites as well as automated searches and, thus, often contain websites that have been incorrectly classified. In addition, blunt filtering methods such as IP blocking can knock out large swaths of acceptable websites simply because they are hosted on the same IP address as a site with restricted content.

Section 313 was used by ASIC 10 times during the 2012-2013 financial year to block websites which it deemed to be advertising or promoting ‘investment scams’ to Australian website users¹⁶ and ASIC admitted to inadvertently blocking 250,000 legitimate websites from public access.¹⁷

Other practical problems are that:

- the worst content, like child pornography, tends to be shared peer to peer and not to be available through public websites, therefore blocking is relatively useless in stopping the dissemination of such material;¹⁸
- research shows that internet filtering does not work and is easy to circumvent using simple techniques such as use of a Virtual Private Network (VPN) and proxies;

¹² Open Rights Group, “Counter Terrorism Internet Referral Unit”, in the context of the operation of the *Terrorism Act 2006*, <https://wiki.openrightsgroup.org/wiki/Counter_Terrorism_Internet_Referral_Unit> accessed 19 August 2014, citing UK Minister of State James Brokenshire, Hansard, House of Commons, 2 April 2014, Column 948, <http://www.publications.parliament.uk/pa/cm201314/cmhansrd/cm140402/debtext/140402-0003.htm#140402-0003.htm_snew12> accessed 20 August 2014

¹³ *Thomas v Mowbray* (2007) 233 CLR 307, 507-9 (Callinan J).

¹⁴ Craddock, op cit, p 27.

¹⁵ OpenNet Initiative, “About Filtering”, op cit

¹⁶ Ben Grubb, “How ASIC’s attempt to block one website took down 250,000”, *Sydney Morning Herald* (5 June 2013), <<http://www.smh.com.au/digital-life/digital-life-news/how-asics-attempt-to-block-one-website-took-down-250000-20130605-2np6v.html>> accessed 20 August 2014.

¹⁷ Ibid. Craddock notes that this could constitute a tort: op cit, p 30.

¹⁸ Craddock, op cit, p 26, referring to blocking and filtering as ‘technologically outdated.’

- Keyword/image blocking, which blocks access to websites based on the words found in URLs or blocks searches involving blacklisted terms or images, is often inaccurate and catches legitimate sites. In the United Kingdom, “nearly one in five of the most visited sites on the internet are being blocked by the adult content filters installed on Britain’s broadband and mobile networks... A Porsche car dealership, two feminist websites, a blog on the Syrian War and the Guido Fawkes political site are among the domains that have fallen foul of the recently installed filters.”¹⁹

3.3 Negative Impact upon human rights

As a result of the issues referred to in this section, section 313 both in its current and potential operation has an inappropriate impact on Australians’ privacy rights and rights to freedom of expression and communication, contrary to the *International Covenant on Civil and Political Rights* (‘ICCPR’) to which Australia is a party, and which informs Australian law. Article 19 protects freedom of expression and contemplates limits to freedom of expression only to the extent: “provided by law and ... necessary: (a) For respect of the rights or reputations of others; and (b) For the protection of national security or of public order (*ordre public*), or of public health or morals.” Article 17 provides that: “No one shall be subjected to arbitrary or unlawful interference with his privacy”. How these principles should be applied to the internet environment is spelt out further in the *International Principles on the Application of Human Rights to Communications Surveillance* considered at the end of this document.

ALHR submits that international law places an obligation on the State to:

- protect individual privacy; and
- justify the legitimacy of any proposed restrictions on freedom of speech and communication;

and that the current wording of section 313 is so broad that it breaches the International Principles and places Australia in breach of its obligations under the ICCPR.

4. Transparency and Accountability

4.1 Background

While the Terms of Reference ask: ‘what are the most appropriate transparency and accountability measures *that should accompany such requests*, taking into account the nature of the online service being dealt with?’ it is submitted that transparency and accountability are fundamental to all the questions raised by the Terms of Reference. It is also unclear what the reference to measures ‘accompanying’ a request to a carrier could mean unless it refers to a warrant or court order (with which interpretation we are in agreement).

A ‘transparency and accountability measure’ in the legal context is an action, procedure, or a particular arrangement intended as a means to achieve a particular end²⁰ (**‘Measure’**), such as ensuring that:

- a decision is ‘open to scrutiny’ (**‘Transparency’**);²¹ and
- an actor has an *obligation* to explain and justify his or her conduct to some significant other,²² where that obligation specifies:
 - to *whom* the decision-maker is accountable;
 - by what *process*;
 - according to what *standards*; and
 - involving what *effects* (**‘Accountability’**).²³

‘Transparency’ and ‘accountability’ can apply at different levels and with slightly different meanings: (1) in the sense of whether internet service disruption is obvious or ‘transparent’ to all stakeholders including service providers and internet users, (2) in the legal context of whether the actions of authorities under section 313 are open to judicial review, and (3) in the sense of whether the policies and procedures that are applied by

¹⁹ Juliet Garside, “Internet filters blocking one in five most-popular websites”, *The Guardian* (3 July 2014) <<http://www.theguardian.com/technology/2014/jul/02/internet-filters-blocking-popular-websites-guido-jezebel>> accessed 20 August 2014.

²⁰ *Macquarie Dictionary*

²¹ George Argyrous, ‘Evidence Based Policy: Principles of Transparency and Accountability’ *Australian Journal of Public Administration* (71)(4) 457, 459.

²² *Ibid.*

²³ J Mashaw, ‘Accountability and Institutional Design: Some Thoughts on the Grammar of Governance’, in M Dowdle (ed) *Public Accountability: Designs, Dilemmas and Experiences* (CUP) 118.

authorities in disrupting internet usage are open to public scrutiny, including in that procedures and statistics are publicly available.

The *International Principles* support the notion that States should be transparent at all these levels and in all these senses about the use and scope of communications surveillance/disruption laws so as to draw a proper balance between the potential infringement of human rights and State interests. States should publish information on the specific number of surveillance/disruption requests approved and rejected and the specific number of individuals affected. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the relevant laws. States should not interfere with service providers who publish the procedures they apply when complying with State requests for communications surveillance or disruption.

4.2 Changes in transparency under Australian legislation

Under Australia's Westminster system of government, section 75 of the Constitution confers on the High Court of Australia original jurisdiction in matters in which any of the three administrative law remedies that the Constitution names (the writs of mandamus, prohibition, or an injunction) are sought against an officer of the Commonwealth;²⁴ and in matters 'in which the Commonwealth, or a person suing or being sued on behalf of the Commonwealth, is a party'.²⁵ Accordingly, Australia's constitutional framers guaranteed that 'there is an entrenched jurisdiction to deal with the validity of Commonwealth legislation and executive action';²⁶ and 'there would be a jurisdiction capable of restraining officers of the Commonwealth from exceeding Federal power'.²⁷

An increased focus in respect of 'national security' in Australia in recent decades has however involved a departure from previous review and public transparency standards. In response to 9/11, Australian legislation authorised the interception of non-suspects' communication,²⁸ allowed the Attorney General to issue warrants on the application of ASIO's Director General;²⁹ introduced a new regime allowing the government to intercept 'stored communications' – that is, communications sent across a telecommunications system and accessible to the intended recipient;³⁰ and allowed the Director-General of ASIO to apply to the Attorney-General for questioning and detention warrants.³¹

Effectively, Australia:

- moved from largely relying on Australia's criminal law (with all its tested procedural safeguards) in promoting national security, to relying on a system that uses special provisions to target classes of people that may include innocent bystanders;³²
- moved from allowing judges to authorise the interception of communications to and from a telecommunications service in specific circumstances – where there were reasonable grounds for suspecting that a particular person was likely to use the service, and the information obtained was likely to assist the investigation of an offence in which the person involved – to a system that allows elected officials to issue such warrants on the ASIO Director-General's application;
- expanded the scope of communications that the Government could monitor for the purposes of national security protection; and
- included non-suspects within the class of persons the government could monitor.

ALHR submits that future legislation should be used to implement transparency and accountability measures and rebalance Australia's review and public transparency standards, in ways that other methods cannot.

²⁴ Section 75(v).

²⁵ Section 75(iii).

²⁶ L. Zines, 'Federal, Associated and Accrued Jurisdiction', in B. Opeskin and F. Wheeler (eds), 265, 269; Dixon J in *Australian Communist Party* at 193 cited in Simon Evans, 'Continuity and Flexibility: Executive Power in Australia' in Paul Craig and Adam Tomkins (ed), *The Executive and Public Law: Power and Accountability in Comparative Perspective* 90.

²⁷ *Bank of NSW v. Commonwealth* Dixon (1948) 76 CLR 1, 363; *Deputy Commissioner of Taxation v. Richard Walter* (1994) 183 CLR 168, 178–9 cited in Simon Evans, 'Continuity and Flexibility: Executive Power in Australia' in Paul Craig and Adam Tomkins (ed), *The Executive and Public Law: Power and Accountability in Comparative Perspective* 90.

²⁸ *Telecommunications (Interception) Amendment Act 2006* (Cth) sections 9 and 46.

²⁹ *Ibid*, section 9(1).

³⁰ *Ibid*, section 110.

³¹ *Australian Security Intelligence Organisation Act 1979* (Cth) Part III div III.

³² David Hume and George Williams, 'Who's Listening? Intercepting the telephone calls, emails and SMS's of innocent people' (2006) 31 *Alternative Law Journal*, 211; Kent Roach, *The 9/11 Effect: Comparative Counter-terrorism* (Cambridge University Press, 2011) 317; George Williams, 'A Decade of Australian Anti-terror Laws' (2011) 35 *Melbourne University Law Review* 1137; 1140; and George Williams, 'One year On: Australia's Legal Response to September 11' (2002) *Alternative Law Journal* 212.

4.3 Transparency, accountability and section 313

Currently, there is no legislatively mandated transparency or accountability in relation to section 313. The section has, broadly speaking, two branches:

- the 'crime prevention' duty on carriers, carriage service providers and carriage service intermediaries, encapsulated in subsections 313(1) and 313(2); and
- the general duty to assist officers and authorities of the Commonwealth and of the States and Territories in conducting law enforcement duties and the like, imposed by subsections 313(3) and 313(4).

From a transparency perspective, the Act does not:

- impose any limits on the agencies that might request assistance under subsections 313(3) and 313(4), or who or what entity might suggest preventative action be taken pursuant to subsections 313(1) and 313(2);
- provide for any reporting requirement for the number and nature of requests made under subsections 313(3) and 313(4), or reporting on how subsections 313(1) and 313(2) are used by agencies;
- prescribe for any level of independent oversight of agency use of this section;
- prescribe any formal procedure for agency use of this section (eg. no formal powers are conferred on agencies to compel compliance with the duties, no formal warrant or application process is outlined);
- provide for detailed and transparent notice to end-users where preventative action may result in the blocking of access to internet content.³³

The lack of transparency in the section as it currently stands raises concerns as to the protection of individuals' privacy and freedom of communication, and the potential for unchecked agency pressuring of ISPs to block websites.

In submissions to the Senate Standing Committees on Legal and Constitutional Affairs inquiry into the comprehensive revision of the *Telecommunications (Interception and Access) Act 1979* (TIA Act), several organisations voiced the same concerns.

The Australian Privacy Foundation noted that the range of agencies that can use section 313 is greater than those that are permitted to use powers under the TIA Act, and that requests made pursuant to the 'crime prevention' duty are likely to be informal, difficult to detect and unlikely to be reported on.³⁴

Internet Service Provider (ISP) iiNet Limited also voiced concern specifically about agencies' use of section 313 to force ISPs to block websites. iiNet's submission highlighted the lack of transparency, accountability and lack of oversight in this process, and outlined that in effect, the onus is placed on providers to evaluate the legitimacy of the agency's request to the ISP.³⁵

As of November 2011, the Australian Law Reform Commission notes that the AFP had issued five section 313 requests to Australian ISPs, implying that five Australian ISPs were voluntarily filtering the INTERPOL blacklist at the ISP-level. There is no requirement for the ISPs to report their statistics, but for the period 1 July–15 October 2011, says the ALRC, Telstra reported that there had been in excess of 84,000 redirections via its network.³⁶

Accordingly, the only apparent process, accountability or oversight in agency use of section 313 rests upon the policies of the requesting agencies (which are not available to the public), and the internal policies of ISPs in dealing with such requests (which are not generally available to the public either).

ALHR is of the view that this current state of affairs is unsatisfactory and the lack of transparency leaves unchecked potential infringements on the privacy rights and rights to freedom of expression and communication of individuals.

³³ See Craddock, op cit, p 33 re failures to notify end users.

³⁴ Australian Privacy Foundation, Submission to the Senate Standing Committees on Legal and Constitutional Affairs inquiry into the comprehensive revision of the *Telecommunications (Interception and Access) Act 1979* <<http://www.aph.gov.au/DocumentStore.ashx?id=bd5ef08a-10e7-460c-8651-9be5d3bdf822&subId=205671>> accessed on 20 August 2014

³⁵ iiNet Limited, Submission to the Senate Standing Committees on Legal and Constitutional Affairs inquiry into the comprehensive revision of the *Telecommunications (Interception and Access) Act 1979* <<http://www.aph.gov.au/DocumentStore.ashx?id=cd64d063-5791-4336-8606-0ee36926b8f9&subId=206461>> accessed on 20 August 2014

³⁶ ALRC Report 118 Classification – Content Regulation and Convergent Media, ALRC 2012 [12.74] <<http://www.alrc.gov.au/publications/12-prohibiting-content/prohibitions-online>> accessed on 20 August 2014

5. Modern practices in other countries

“Overall, Australian Internet regulations are significantly stricter than those of New Zealand and much of the Western world” – OpenNet Initiative³⁷

“France yesterday put in its bid for an unlikely prize, becoming the first western country to make even Australia look liberal when it comes to state powers of internet censorship.”³⁸

OpenNet Initiative has commented with concern that Australia’s Internet censorship regime is strikingly severe relative to both its neighbor and similar Western states, and it is helping to push the normative boundaries of filtering for an industrialized democratic state in a negative direction.³⁹

Europe

The European Data Protection Supervisor has said that any requirement for hosts to “prevent illegal content” should not place responsibility on those service providers to generally monitor information that is transmitted or stored on their service to identify illegal activity. In addition such a general monitoring obligation is contrary to the UK E-Commerce Directive, as the fundamental principle underlying the liability provisions of the directive is that an Internet intermediary (an ISP) should not be held liable for the transmission, hosting or caching of information.⁴⁰ The European Court of Justice has ruled against initiatives requiring internet service providers⁴¹ and social networks⁴² to install a filtering system to prevent customers using websites that infringe intellectual property rights.

The 2012 European Court of Human Rights decision in *Yildirim v Turkey*⁴³ helpfully compares the mechanisms for website blocking in place in various European states. Judge Pinto de Albuquerque provided an 11-point framework for website blocking legislation compatible with the European Convention on Human Rights, which required such legislation to contain:

1. a definition of the categories of persons and institutions liable to have their publications blocked;
2. a definition of the categories of blocking orders, such as blocking of entire websites, IP addresses, ports, network protocols or types of use, like social networking;
3. a provision on the territorial ambit of the blocking order;
4. a limit on the duration of the blocking order;
5. an indication of the “interests”, in the sense of one or more of those included in Article 10 (2) of the Convention⁴⁴, that may justify the blocking order;
6. observance of the criterion of proportionality;
7. compliance with the principle of necessity, which enables an assessment to be made as to whether the interference with freedom of expression adequately advances the “interests” pursued and goes no further than is necessary to meet the said “social need”;
8. a definition of the authorities competent to issue a reasoned blocking order;
9. a procedure to be followed for the issuance of that order, which includes the examination by the competent authority of the evidence supporting the request for a blocking order and the hearing of evidence from the affected person or institution, unless this is impossible or incompatible with the “interests” pursued;
10. notification of the blocking order and the grounds for it to the persons or institutions affected; and
11. a judicial appeal procedure against the blocking order.

³⁷ OpenNet Initiative, “Australia and New Zealand” op cit.

³⁸ Jane Fae Ozimek, “France leapfrogs past Australia in Big Brother stakes,” *The Register* (17 Feb 2010), <http://www.theregister.co.uk/2010/02/17/france_ip_law/>, accessed 8 August 2014

³⁹ OpenNet Initiative, “Australia and New Zealand” op cit.

⁴⁰ Craddock, pp 27-28.

⁴¹ *Scarlet Extended SA v Societe Belge des Auteurs, Compositeurs et Editeurs SCRL (SABAM)* (24 November 2011), Case C-70/10, see <<http://curia.europa.eu/juris/liste.jsf?language=en&num=C-70/10>> accessed 20 August 2014

⁴² *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* (16 February 2012), Case C-360/10, see <<http://curia.europa.eu/juris/document/document.jsf?sessionid=9ea7d2dc30dbf6556d513fec47108276a0c7a297f9e7.e34KaxiLc3qMb40Rch0SaxqTc390?text=&docid=119512&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=158263>> accessed 20 August 2014

⁴³ *Yildirim v Turkey* ECHR No 3111/10 (18 December 2012) < [http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-115705#{"itemid":\["001-115705"\]}](http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-115705#{)> accessed 20 August 2014

⁴⁴ Article 10(2) provides that the freedom “may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.”

In 2010, Germany and France passed laws requiring that “ISPs adopt a blacklist maintained by a governmental organisation.” Concerns have been raised that such a list might be expanded to include other undesirable content, without democratic control of these changes.⁴⁵

UK

In the United Kingdom, directions to ISP providers to block specific websites that infringe intellectual property have been upheld in the 2011 case concerning ‘Newzbin2’ on the basis that they were narrowly targeted.⁴⁶

Internet content that incites or glorifies terrorist acts can be removed by the Counter Terrorism Internet Referral Unit (CTIRU) under Section 3 of the *Terrorism Act 2006*.⁴⁷ Where content is not hosted under the UK jurisdiction, sites hosting “extremist” content may be blocked by UK ISPs. A list of sites and search terms provided by the Counter Terrorism Internet Referral Unit⁴⁸ are blocked on networks that subscribe to the list. By June 2013 this list contained almost 1,000 addresses.⁴⁹ The amount of material removed in accordance with CTIRU requests appears to be increasing exponentially:

From February 2010 to 2013 [CTIRU] had requested removal of “approximately 6,500 pieces of online content”[1] “Figures for April 2012 to March 2013 stand at 3,538 pieces of online content removed.”[2] By December 2013 had “removed more than 18,000 pieces of illegal material”,[3] and by March 2014 “it has removed more than 26,000 pieces of illegal terrorist material online”[4], “29,000 pieces” by April 2014.[5], “34,000 pieces” by June 2014[6], “40,000 items” by July 2014[7][8].⁵⁰

Legal action has been launched in the UK against the *Data Retention and Investigatory Powers Act 2014* which was introduced to parliament as an emergency bill and passed through all scrutiny stages within a week. The case will argue the legislation is incompatible with Article 8 of the European Convention on Human Rights and Article 7 of the European Charter of Fundamental Rights, which calls for the respect for private and family life and protection of personal data.⁵¹

USA

ISPs have not been the main target of filtering legislation in the USA. There has instead been a focus on requiring mandatory filtering for schools and libraries to obtain funding.⁵² While some of these filters have opt-out mechanisms, there is considerable concern that their use has been over-broad, thus restricting childrens’ education and communication.⁵³

In 1986 the US Federal Government passed the Electronic Communications Privacy Act 1986 (‘ECPA’) as a form of statutory protection to broaden the effectiveness of the Constitutional right to privacy, following a number of decisions which limited the Fourth Amendment right to privacy at the expense of government access to electronic data.⁵⁴ In accordance with the Act, if the government seeks to obtain electronic data it must:

- obtain a warrant issued under the Federal Rules of Criminal Procedure or state equivalent; or
- give prior notice to the customer if the government uses an administrative subpoena, authorised by Federal or State statute, or a Federal or State grand jury or trial subpoena; or
- obtain a court order, by showing the court that there are reasonable grounds to believe that the contents of the data are relevant to an ongoing criminal investigation.⁵⁵

⁴⁵ Craddock, p 9.

⁴⁶ Open Rights Group, “Newzbin” <<https://wiki.openrightsgroup.org/wiki/Newzbin>> accessed 19 August 2014

⁴⁷ Open Rights Group, “Counter Terrorism Internet Referral Unit”, <https://wiki.openrightsgroup.org/wiki/Counter_Terrorism_Internet_Referral_Unit> accessed 19 August 2014

⁴⁸ Open Rights Group, “Counter Terrorism Internet Referral Unit”, op cit

⁴⁹ Open Rights Group, “Blocking of Extremist Material” <https://wiki.openrightsgroup.org/wiki/Blocking_of_extremist_material> accessed 19 August 2014

⁵⁰ Open Rights Group, “Counter Terrorism Internet Referral Unit”, op cit.

⁵¹ Open Rights Group, “ORG Parliamentary and Policy Update 2014 – w 30”, <https://wiki.openrightsgroup.org/wiki/ORG_parliamentary_and_policy_update/2014-w30> accessed 19 August 2014

⁵² Craddock, op cit, p 10 ff.

⁵³ Deborah Caldwell-Stone, , ‘Filtering and the First Amendment: When is it okay to block speech online?’, *American Libraries*, 2 April 2013, <<http://www.americanlibrariesmagazine.org/article/filtering-and-first-amendment>> accessed 14 August 2014.

⁵⁴ See also Jayni Foley, “Are Google Searches Private? An Originalist Interpretation of the Fourth Amendment In Online Communication Cases”, *Berkeley Technology Law Journal*, (2007) vol. 22 no. 447, pp. 1 – 24 <<http://scholarship.law.berkeley.edu/btlj/vol22/iss1/24/>> accessed 19 August 2014

⁵⁵ Ibid, s 2703(c) and (d).

The court may also authorise that the government provide a delayed notification when issuing a subpoena if the circumstances of the case deem this to be appropriate. In accordance with section 2705(a)(2), the government may provide a delayed notification in circumstances that involve:

- Endangering the life or physical safety of an individual;
- Flight from prosecution;
- Destruction of or tampering with evidence;
- Intimidation of potential witnesses; or
- Otherwise seriously jeopardizing an investigation or unduly delaying a trial.

6. Terms of Reference Questions

6.1 Which government agencies should be permitted to make requests pursuant to section 313 to disrupt online services potentially in breach of Australian law from providing these services to Australians

- (1) No government agency or officer should be permitted to disrupt online services on the basis that they are 'potentially' in breach of Australian law. This is an overbroad interpretation of the current law. Nor should this concept be introduced into section 313 in the future. It should be established before an Australian court or tribunal that a service is in breach of Australian law before any further action can be taken.
- (2) The agencies should be limited to law enforcement agencies. The fewer agencies, the less potential there is for the abuse of such powers. It is quite unacceptable to have all State (which includes Local Council) and Federal agencies able to require disruption of online services, even where they are subject to appropriate restrictions and review, which currently they are not.

6.2 What level of authority should such agencies have in order to make such a request?

We submit that Australian legislation regulating the use of website blocking by statutory agencies or government departments should adhere to a similar framework to that proposed in *Yildirim v Turkey*⁵⁶. In particular, Australia should adopt the requirements to provide a procedure for agencies to obtain a blocking order/warrant, appropriate notification of the order to affected parties and a judicial appeal process, and regular public reporting in order to ensure that transparency measures are adequate. That is:

- Agencies should be authorised by a 'blocking' warrant issued by a court or tribunal in order to make a carrier request. It would seem most appropriate for the Administrative Appeals Tribunal to have the power to approve requests from government agencies (similar to the current situation under the Telecommunications (Interception and Access) Act 1978 where the AAT has the power to issue telecommunications interception warrants and stored communications warrants/named person warrants (real-time intercepts)).⁵⁷
- the warrant provisions of the legislation should include a 'proportionality test';⁵⁸
- the warrant provisions of the legislation should require substantial evidence to be produced of the serious criminal nature of the crime being carried out through the service in question;
- a general obligation should 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 rights being breached.⁵⁹

6.3 [What should be] the [identifying] characteristics of illegal or potentially illegal online services which should be subject to such requests?

Only services established to be involved in serious crimes or that directly incite serious crimes should be covered by carrier requests. The present wording in section 313 (3) that permits carrier requests to protect the public revenue or impose pecuniary penalties is quite inappropriate, and – as mentioned – potential illegality should not be a criterion.

⁵⁶ *Yildirim v Turkey* op cit

⁵⁷ Section 47.

⁵⁸ Blueprint for Free Speech, op cit, p 14 and International Principles, item 5.

⁵⁹ *ibid*

It would be appropriate to look to the same characteristics advocated by the Law Council of Australia in relation to stored communication and telecommunications intercept warrants (that is, that the service is carrying out serious criminal offences and not ‘pre-cursor’ offences).

It is not necessarily appropriate to identify some serious crimes as more worthy of blocking than others, although it may be that the practical effect of blocking some types of websites may be of less effect (because of peer to peer sharing, say, of pornography) than of blocking others (such as hate crime sites).

6.4 What are the most appropriate transparency and accountability measures that should accompany such requests, taking into account the nature of the online service being dealt with?

See paragraphs 1(5), 1(6), section 4 and section 6.2. Again, it is not necessarily appropriate to take into account the nature of the particular crime being addressed, as the same transparency and accountability measures should generally apply, including in case of national security.

Transparency at all stages of the process is desirable, not just at the point of the request.

- (1) The end user should be informed by a ‘stop page’ that they have attempted to access a website that has been blocked.⁶⁰ Stop pages should clearly detail which statutory authority requested the block under section 313 with their contact information and detail the process for the website owner to appeal the application of the block.
- (2) Notifications should be made to the owner of the domain name of the website being blocked. Blocking is not necessarily consistent across ISPs so a site may be visible on one device, but be blocked by other ISPs.⁶¹ There should be clear avenues for appeal of a decision to block a website. Where for extreme national security reasons this is not appropriate, a special advocate should be appointed to represent the owner’s interests.
- (3) If not all ISPs are participating in the particular disruption, consumers should know if their ISP is part of the blocking of their content using section 313. ISPs should be required to notify consumers whether they participate in the blocking, and their policies in that regard, so consumers can make an informed decision as to whether they wish to use that service.
- (4) There should be quarterly/regular reporting available to the public on the website of the government agency managing the requests, as well as an annual report to Parliament (use of section 313 could be covered in the annual reports provided on use of the TIA Act powers which are provided by the Attorney-General’s Department⁶² and the Australian Communications and Media Authority⁶³ and, where relevant, in the annual report of the Inspector- General of Intelligence and Security⁶⁴). Reports should show: the number of websites blocked, which agency requested the block, type of website being blocked, location of server, reasons for decision to use section 313, costs to the Government (including any compensation) and costs to ISPs of implementing and managing the implementation of blocks. Comparative reports over time should be publicly available to show the use of these powers. Reports should also detail the number of complaints made about blocks and the number of blocks removed following the complaint.
- (5) Activities under section 313 should be open to judicial review and inspection by the Ombudsman relevant to the particular agency as well as a special Public Interest Monitor (PIM) (as established in Victoria⁶⁵) to act as an additional level of oversight into the issuing of interception warrants. There

⁶⁰ See Interpol, Example Stop Page <<http://www.interpol.int/Media/Images/Crime-areas/Crimes-against-children/Stop-page>> accessed 20 August 2014.

⁶¹ Open Rights Group, “Department of Dirty: Overblocking” <<http://www.departmentofdirty.co.uk/overblocking>> accessed 20 August 2014.

⁶² Attorney-General Department’s Annual Report 2012-2013 <<http://www.ag.gov.au/Publications/AnnualReports/Annualreport2012-13/Pages/default.aspx>> accessed 20 August 2014 (Annual reporting on how eligible Commonwealth, State and Territory enforcement agencies use *Telecommunications (Interception and Access) Act 1979*).

⁶³ Australian Communications and Media Authority Annual Report 2012-2013 <<http://acma.gov.au/theACMA/Library/Corporate-library/Corporate-publications/communications-report-2012-13>> accessed 20 August 2014. Includes reporting from ISPs and telcos on disclosures made to law enforcement under the *Telecommunication Act 1997* (133,570) and under the *Telecommunications (Interception and Access) Act 1979* (685,757).

⁶⁴ Inspector- General of Intelligence and Security Annual Report 2012-2013 <http://www.igis.gov.au/annual_report/12-13/pdfs/IGIS_annual_report_12-13.pdf> accessed 20 August 2014.

⁶⁵ *Public Interest Monitor Act 2011* (VIC).

should also be oversight of such requests by a Parliamentary Joint Committee, and an annual report on such requests presented to Parliament.

6.5 What is the best/appropriate method for implementing such measures: a. Legislation, b. Regulations, or c. Government policy?

*'It is the cause for the utmost caution when one arm of government (such as the Executive) seeks the approval of the second arm of government ([such as] the Parliament) to exclude the third arm of government (the Judiciary) from its legitimate role, whatever the alleged efficiency, expediency or integrity of the program put forward in justification.'*⁶⁶

Government policy is not a method that could implement appropriate transparency and accountability measures that should accompany government agencies' requests under section 313 as it does not *oblige* a government decision-maker to explain and justify their conduct to a significant other.

Because Australia's Westminster system of government necessitates that courts can review Executive action; and representative and responsible government, judicially reviewable legislation is the best and most appropriate method for implementing Transparency and Accountability Measures in respect of section 313.

Judicially reviewable legislation provides the following benefits that other measures do not:

- (a) it is open to greater parliamentary scrutiny, and is therefore more transparent, than legislative instruments such as regulations;
- (b) it promotes the rule of law in that:
 - (i) it provides for judicial review, which is neither more nor less than the enforcement of the rule of law over executive action. It is the means by which executive action is prevented from exceeding the powers and functions assigned to the executive by the law;⁶⁷
 - (ii) those exercising executive and administrative powers are as much subject to the law as those who are or may be affected by the exercise of those powers. It follows that, within the limits of their jurisdiction and consistent with their obligation to act judicially, pursuant to judicially reviewable legislation, courts should provide whatever remedies are available and appropriate to ensure that those who possess executive and administrative powers exercise them only in accordance with the laws that govern their exercise. The rule of law requires no less;⁶⁸
 - (iii) in any case, to the extent that another branch of government impedes courts from exercising judicial review of administrative decisions, that non-court branch of government negates the rule of law;⁶⁹
- (c) it may improve decision-making as it 'forces care in administrators and reviewers in their adjudicative process';⁷⁰
- (d) it promotes accountability because:
 - (i) a decision-maker whose ruling is subject to curial oversight is less likely to toe a particular policy line, or succumb to political pressure to decide cases in a particular way; and
 - (ii) the courts offer:
 - (A) security to those who make a bona fide attempt to make findings on the facts and the law as presented; and

⁶⁶ Senate Legal and Constitutional Legislation Committee, *Consideration of Legislation Referred to the Committee: Migration Legislation Amendment (Judicial Review) Bill 1998*, April 1999, 27 citing the Scrutiny of Bills Committee report quoted in *Submission No. 8*, National Council of Churches in Australia, 3, cited in Administrative Review Council Reports, *The Scope of Judicial Review Discussion Paper*, 2003, Part II, Section I <http://www.arc.ag.gov.au/Documents/jrpart2.htm#_ftn15> accessed 20 August 2014.

⁶⁷ *Church of Scientology v Woodward* (1982) 154 CLR 25, 71 per Brennan J cited in Administrative Review Council Reports, *The Scope of Judicial Review Discussion Paper*, 2003, Part II, Section II.

⁶⁸ *Corporation of the City of Enfield v Development Assessment Commission* (2000) 199 CLR 135, 157 per Gaudron J cited in Administrative Review Council Reports, op cit, Part II, Section II.

⁶⁹ The Hon Sir Gerald Brennan, 'The Mechanics of Responsibility in Government' (1999) 58(3) *Australian Journal of Public Administration* 3, 9.

⁷⁰ Mary Crock, 'Privative Clauses and the Rule of Law: The Place of Judicial Review Within the Construct of Australian Democracy', in S Kneebone (ed) *Administrative Law and the Rule of Law: Still Part of the Same Package?*, Australian Institute of Administrative Law, 1999, 57, 80.

- (B) sanctions for those who choose to act on arbitrary or capricious considerations;⁷¹
- (e) unlike measures that are less publicly accessible than judicial review (such as government policy), judicial reviewable legislation enhances community confidence because:
 - (i) tribunals in our administrative system do not establish precedent. In contrast, courts' rulings are of precedential value, and can provide direction regarding obligations that statutes impose upon decision-makers;⁷²
 - (ii) judicial review promotes and protects individual rights by:
 - (A) protecting individuals' right to the review of governments' decisions in a way that the doctrine of ministerial responsibility does not, which is reflected in Australia's comprehensive system of administrative law;⁷³ and
 - (B) judicial review of legislation clarifies the standards that the Commonwealth administration will apply in making decisions that affect individuals in the community's interests. An essential part of judicial review of administrative action has been the progressive development by an independent judiciary of procedural standards of fairness and lawfulness against which one may measure the powers of government officials;⁷⁴ and
- (f) generally, the ousting of judicial review is not a matter that Parliaments should undertake lightly.

Accordingly, legislation would implement transparency and accountability measures that should accompany requests under section 313, and rebalance Australia's review and public transparency standards by allowing greater parliamentary scrutiny of section 313; and open, judicial, impartial, and independent supervision of section 313.

ALHR

ALHR was established in 1993. ALHR is a network of Australian law students and lawyers active in practising and promoting awareness of international human rights. ALHR has a national membership of over 2600 people, with active National, State and Territory committees. Through training, information, submissions and networking, ALHR promotes the practice of human rights law in Australia. ALHR has extensive experience and expertise in the principles and practice of international law, and human rights law in Australia.

Yours faithfully

Roslyn Cook
Vice-President
Australian Lawyers for Human Rights

Contributors: Rosanna Cuppaidge, Michelle Meares, Brendan Donohue, Maja Doma, Mila Dragicevic, Ashanthi Jayasekera, Georgia Murphy-Haste, James Souter, Shavindi Welivitiya, Carly Nyst, Tamsin Clarke

⁷¹ Ibid.

⁷² Administrative Review Council Reports, op cit, Part II, Section II, [2.8].

⁷³ *R v Toohey; Ex parte Northern Land Council* (1981) 151 CLR 170, 222 per Mason CJ.

⁷⁴ Administrative Review Council, *Review of the Administrative Decisions (Judicial Review) Act: The Ambit of the Act*, Report No 32, 1989, 6.

**Annexure to ALHR Submission in relation to section 313 of the Telecommunications Act 1997:
Does section 313 meet the International Principles on the Application of Human Rights to Communications Surveillance?**

	International Principle (summarised)	Section 313
1	LEGALITY: Relevant legislation must meet a standard of clarity and precision sufficient to foresee its application.	Very vaguely worded and open-ended. Not sufficiently specific. Foreseeability is linked to transparency and the principles guiding the creation and maintenance of any blacklist should be made available to this end. ⁷⁵
2	LEGITIMATE AIM: Relevant legislation must: <ul style="list-style-type: none"> be intended to achieve: <ul style="list-style-type: none"> a legitimate aim that corresponds to a predominantly important legal interest necessary in a democratic society not be applied in a discriminatory manner. 	While some uses of the section (eg protecting against the dissemination and use of illegal data such as child pornography) are a legitimate aim, the legislation is too broadly drafted. Freedom of expression is arguably an interest that is more necessary in a democratic society than protection of citizens via disrupting the free flow of communication. Unintended blocking of legitimate sites points to the overbroad nature of section 313.
3	NECESSITY: Surveillance laws must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim. Communications Surveillance must only be conducted when it is: <ul style="list-style-type: none"> the only means of achieving a legitimate aim, the means least likely to infringe upon human rights. 	That section 313 appears to be used or to be intended to be used not only against proved criminal activity but ‘potential’ criminal activity demonstrates that it is not limited to what is strictly necessary to achieve the aim of blocking sites containing illegal activity. Service disruption is not the method least intrusive to human rights. Calling on the removal of illegal material via a two way dialogue – and, if necessary, through international cooperation - would appear more appropriate and effective ⁷⁶ than the unintended effect often achieved of blocking swathes of legitimate sites. For this criteria to be met, one must be able to show that the measures taken are effective in achieving the objectives. Underblocking and overblocking bring the scope of the section into question.
4	ADEQUACY: Any instance of Communications Surveillance authorised by law must be appropriate to fulfil the specific Legitimate Aim identified.	There needs to be a specific justification for the blocking or filtering of Internet content. Arguably, data disruption is not appropriate or adequate to fulfill the stated aim of protection from illegal activities.
5	PROPORTIONALITY: Decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights. Prior to conducting Communications Surveillance, the State must establish the	Under section 313 there is no balance between privacy in communications and legal enforcement and no requirement for any government authority to prove each of these points or meet these targets before proceeding with the data disruption.

⁷⁵ Craddock, op cit, pp 20 and 21.

⁷⁶ Craddock, op cit, p 27.

	International Principle (summarised)	Section 313
	<p>following to a Competent Judicial Authority:</p> <ul style="list-style-type: none"> • There is a high degree of probability that a serious crime or specific threat to a Legitimate Aim has been or will be carried out, and; • There is a high degree of probability that evidence of a serious crime or specific threat to a legitimate aim would be obtained by accessing the protected information sought, and; • Other less invasive techniques have been exhausted or would be futile and; • Information accessed will be confined to that which is relevant and material; and • Any excess information collected will not be retained, but destroyed or returned; and • Information will be accessed only by the specified authority and used only for the approved purpose; and • That the surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or fundamental freedoms. 	<p>If it can be demonstrated that the filtering is necessary and appropriate (which is in question as mentioned), as well as being effective in achieving its objective, then the interference with human rights must still be proportionate to the risk posed by the relevant criminal activity in question.</p> <p>Case studies of comparable Western democracies show increasing concern regarding the human rights implications of ISP address blocking (Refer to section 5).</p>
6	<p>COMPETENT JUDICIAL AUTHORITY: Determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent which is:</p> <ol style="list-style-type: none"> 1. Separate and independent from the authorities conducting Communications Surveillance; 2. Knowledgeable of issues surrounding the legality of Communications Surveillance, the technologies used and human rights implications; and <p>has adequate resources.</p>	<p>Whilst the judiciary is separate to government agencies like ASIO and provides a check on their power, much legislation restricts judicial review and, as mentioned, section 313 does not allow for judicial consent to be obtained <u>before</u> the measures are taken.</p>
7	<p>DUE PROCESS: Due process requires that States respect and guarantee individuals' human rights by ensuring the procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public.</p>	<p>Following the right to procedural fairness, an affected individual should be afforded the right to present their case before their service is disrupted. Section 313 makes no provision for this. Nor are the procedures according to which section 313 is applied made public.</p>
8	<p>USER NOTIFICATION: Those under surveillance should be notified with enough time and information to enable them to challenge the decision or seek other</p>	<p>There are no equivalent provisions under section 313. Central to our judicial system is the principle of a fair hearing. This applies when an administrative</p>

	International Principle (summarised)	Section 313
	<p>remedies. Access to the evidence against them should be made available.</p> <p>Delay in notification is only justified in limited circumstances eg</p> <ol style="list-style-type: none"> 1. notification would seriously jeopardise the purpose of the Communications Surveillance, 2. an imminent risk of danger to human life; 3. authorisation to delay notification is granted by a Competent Judicial Authority and the party affected is notified as soon as a Competent Judicial Authority determines the risk is lifted. <p>The obligation to give notice rests with the State. However, communications service providers should be free to notify individuals of the Communications Surveillance, voluntarily or upon request.</p>	<p>decision affects a person's rights, interests or legitimate expectations in a direct and immediate way⁷⁷. Here an individual's interest in freedom of communication is affected and thus judicial review is appropriate.</p> <p>In terms of the first point, under the <i>ASIO Act (1979) (Cth)</i> ASIO can make Adverse Security Assessments⁷⁸. If an ASA is made the right to disclosure of critical issues can be eroded. This system trusts ASIO as the final arbiter, rather than the judiciary and strikes at the heart of the fair hearing rule central to our judicial system.</p>
9	<p>TRANSPARENCY: States should be transparent about the use and scope of Communications Surveillance laws. They should publish information on the specific number of surveillance requests approved and rejected and the specific number of individuals affected. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the relevant laws. States should not interfere with service providers who publish the procedures they apply when complying with State requests for Communications Surveillance.</p>	<p>Section 313 has no such requirements and it is not government practice to provide such information.</p>
10	<p>PUBLIC OVERSIGHT: States should establish independent oversight mechanisms to ensure transparency and accountability of Communications Surveillance with authority:</p> <ul style="list-style-type: none"> • To access all information about State actions, including, where appropriate, access to secret or classified information • To assess whether the State is making legitimate use of its lawful capabilities; • To evaluate whether the State has been accurately publishing information in accordance with its Transparency obligations • To publish periodic reports • To make public determinations as to the lawfulness of those actions. 	<p>No such mechanisms appear to exist in relation to section 313</p>
11	<p>INTEGRITY OF COMMUNICATIONS AND SYSTEMS: In order to ensure the integrity, security and privacy of communications systems, States should not compel service providers or hardware or software vendors to build surveillance or monitoring</p>	<p>While section 313 could potentially be used for such purposes, we consider here only the issue of blocking, in accordance with the Terms of Reference, to which this item is not relevant.</p>

⁷⁷ *Kioa v West* (1985) 159 CLR 550 [584]

⁷⁸ *ASIO Act (1979) (Cth)* s35

	International Principle (summarised)	Section 313
	<p>capability into their systems, or to collect or retain particular information purely for State Surveillance purposes.</p> <p>Data retention or collection should never be required of service providers. Individuals have the right to express themselves anonymously. States should therefore refrain from compelling the identification of users.</p>	
12	<p>SAFEGUARDS FOR INTERNATIONAL COOPERATION: The mutual legal assistance treaties (MLATs) and other agreements entered into by States should ensure that, where the laws of more than one state could apply to Communications Surveillance, the standard with the higher level of protection for individuals is applied. Where states seek assistance for law enforcement purposes, the principle of dual criminality should be applied. States may not use mutual legal assistance processes and foreign requests for Protected Information to circumvent domestic legal restrictions on Communications Surveillance.</p> <p>Mutual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees of procedural fairness.</p>	<p>Section 313 has no such requirements and it is not government practice to provide such information.</p>
13	<p>SAFEGUARDS AGAINST ILLEGITIMATE ACCESS AND RIGHT TO EFFECTIVE REMEDY: States should enact legislation criminalising illegal Communications Surveillance by public or private actors. The law should provide civil and criminal penalties, protections for whistleblowers, and avenues for redress by those affected. Laws should stipulate that any information obtained in a manner that is inconsistent with these principles is inadmissible as evidence, as is any evidence derivative of such information.</p> <p>Laws are also needed to ensure that material obtained through legal Surveillance is:</p> <ul style="list-style-type: none"> • Only used for the purpose for which it was obtained, and • The material must not be retained, but destroyed or returned to those affected. 	<p>Section 313 has no such requirements.</p> <p>There is undeniable potential for abuse of this section, resulting in harm that could outweigh the type of harm it seeks to eradicate. With no specific penalties to complement an abuse of the power given by section 313, its reach is disproportionate and its overarching aim is greatly weakened.</p>