Freedom House

Australia

	2013	2014
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	2	2
Limits on Content (0-35)	5	5
Violations of User Rights (0-40)	10	10
TOTAL* (0-100)	**17**	**17**

* 0=most free, 100=least free

Population:	23.1 million
Internet Penetration 2013:	83 percent
Social Media/ICT Apps Blocked:	No
Political/Social Content Blocked:	No
Bloggers/ICT Users Arrested:	No
Press Freedom 2014 Status:	Free

Key Developments: May 2013 – May 2014

- Broadband access continued to expand for online users as the National Broadband Network reached more rural and remote communities (see **Obstacles to Access**).
- Concerns over ISP filtering practices continued in response to the government's consideration of a graduated response scheme and the blocking of piracy websites (see **Limits on Content**).
- Revelations regarding global surveillance and the retention of communications data by intelligence agencies, and legislative proposals in the Australian parliament that could increase government surveillance, raised concerns regarding internet users' right to privacy and freedom of expression (see **Violations of User Rights**).

Introduction

Australia enjoys affordable, high-quality access to the internet and other digital media, and this access has continued to expand over the past few years with the rollout of the National Broadband Network. However, recent amendments to surveillance legislation and proposals to implement censorship through directives to internet service providers (ISPs) have raised concerns about privacy and freedom of expression.[1]

Additionally, in late 2012 Australia acceded to the Council of Europe's Convention on Cybercrime, which brought into effect a number of obligations for ISPs to monitor, preserve, and store user data. However, Australia's legislation goes beyond the requirements set out in the Convention by requiring longer retention timelines for foreign preservation notices, and requiring ISPs to cooperate with any serious crime being investigated in Australia or overseas.

Obstacles to Access

Australia had an internet penetration rate of approximately 83 percent as of December 2013, according to the International Telecommunication Union.[2] From 2012 to 2013, there was a 2 percent increase in internet subscriptions, with 12.4 million internet subscribers in Australia (excluding internet connections enabled through mobile phone handsets) and 19.6 million mobile handset subscribers.[3] The internet penetration rate is expected to steadily increase over the next five years with the implementation of the National Broadband Network (NBN), which includes expanded wireless and satellite services in rural communities. Although internet access is widely available in locations such as libraries, educational institutions, and internet cafes, Australians predominantly access the internet from home, work, the homes of friends and families and increasingly through mobile phones.[4]

Access to the internet and other digital media is widespread in Australia. Australians have a number of internet connection options, including ADSL, ADSL 2+, wireless, cable, satellite, and dial-up.[5] Wireless systems can reach 99 percent of the population, while satellite capabilities are able to reach 100 percent.[6] As of December 2013, over 98 percent of internet connections were broadband, while the number of dial-up connections has declined to 2 percent.[7] Once implemented, the NBN

1 For a comprehensive overview of the legislative history of censorship in Australia see Libertus.net, "Australia's Internet Censorship System," accessed June 2010, http://libertus.net/censor/netcensor.html. See also Australian Privacy Foundation, accessed June 2010, http://www.privacy.org.au.

2 International Telecommunication Union, "Percentage of Individuals Using the Internet," accessed July 2014, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

3 Australian Bureau of Statistics, "8153.0 – Internet Activity, Australia, December 2013: Mobile Handset Subscribers," May 1, 2014, http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/8153.0Chapter8December%202013.

4 Australian Bureau of Statistics, "Household Use of Information Technology, Australia, 2012-2013," accessed May 2014, http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/DE28AB7779067AACCA257C89000E3F98?opendocument.

5 Australian Communications and Media Authority (ACMA), *Communications Report, 2008–09* (Canberra: ACMA, 2009), http://www.acma.gov.au/webwr/_assets/main/lib311252/08-09_comms_report.pdf.
Australian Communications and Media Authority (ACMA), *Communications Report, 2010-11* (Canberra: ACMA, 2011), http://www.acma.gov.au/webwr/_assets/main/lib410148/communications_report_2010-11.pdf.

6 Australian Bureau of Statistics, "8153.0 – Internet Activity, Australia, December 2013: Type of Access Connection," May 1, 2014, http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/8153.0Chapter3December%202013.

7 Ibid.

will eliminate the need for any remaining dial-up connections and make high-speed broadband available to Australians in remote and rural areas.[8]

Roughly half of all Australians have access to broadband speeds of 256 Kbps or greater. While there are still parts of Australia experiencing slower broadband speeds (1.5 Mbps to 8 Mbps), there has been a steady increase since 2012 in connections with faster speeds.[9] Under the revised NBN roll-out, it is expected that two-thirds of Australian's will have download speeds of nearly 100 Mbps by 2019.[10]

Age is a significant indicator of internet use: 97 percent of Australians between the ages of 15 and 17 are internet users, compared to only 46 percent of those over 65 years old.

According to the 2011 Census, 63 percent of Aboriginal and Torres Strait Islanders report having an internet connection, compared with 77 percent of other households.[11] Of those with internet access, 85 percent access the internet through broadband connections.[12] The overall mobile phone penetration rate in Aboriginal communities is unknown.

According to the International Telecommunication Union, Australia had a mobile phone penetration rate of 108.6 percent, or 24.9 million subscriptions, in 2013.[13] Third generation (3G) mobile services are the driving force behind the recent growth, with 25.8 million mobile subscriptions operating in 2013.[14]

Internet access is affordable for most Australians. The government subsidizes satellite phones and internet connections for individuals and small businesses in remote and rural areas, where internet affordability is not comparable to that in metropolitan areas.[15] Major ISPs such as Telstra also continue to offer financial assistance for internet connections to low-income families.[16]

There are no limits to the amount of bandwidth that ISPs can supply. While the government does not place restrictions on bandwidth, ISPs are free to adopt internal market practices of traffic shaping. Some Australian ISPs and mobile service providers practice traffic shaping (also known as data shaping) under what are known as fair-use policies. If a customer is a heavy peer-to-peer

8 Australian Government National Broadband Network, "NBN Key Questions and Answers," accessed June 2010. http://www.nbn.gov.au/content/nbn-key-questions-and-answers-faqs.

9 Australian Bureau of Statistics, "8153.0 – Internet Activity, Australia, December 2013: Type of Access Connection", accessed 15 May 2014, http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/E9B5934F326E48EECA257CB300132152?opendocument

10 Australian Government Department of Communications, National Broadband Network, accessed May 1, 2014, http://www.communications.gov.au/broadband/national_broadband_network#nbnreview.

11 Australian Bureau of Statistics, "Census of Population and Housing: Characteristics of Aboriginal and Torres Strait Islander Australians, 2011," accessed May 2014, http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/2076.0main+features702011.

12 Australian Bureau of Statistics, "Census of Population and Housing: Characteristics of Aboriginal and Torres Strait Islander Australians, 2011," accessed May 2014, http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/2076.0main+features702011.

13 International Telecommunication Union (ITU), "Mobile-cellular subscriptions," 2013, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

14 Australian Communications and Media Authority (ACMA), Communications Report, 2012-2012 (Canberra: ACMA, 2013), http://www.acma.gov.au/~/media/Communications%20Analysis/Comms%20Report%202012%2013/PDF/ACMA%20Communications%20report%20201213_WEB%20pdf.pdf.

15 Rural Broadband, "Welcome," accessed June 2010, http://www.ruralbroadband.com.au.

16 Telstra, *Telstra Sustainability Report 2011*, accessed March 2013, http://www.telstra.com.au/abouttelstra/download/document/2011-sustainability-report.pdf.

user, the internet connectivity for those activities will be slowed down to free bandwidth for other applications.[17]

Like most other industrialized nations, Australia hosts a competitive market for internet access, with 76 providers as of December 2013, nine of which are very large ISPs (over 100,000 subscribers), another 19 large ISPs (with 10,001 to 100,000 subscribers), and 48 medium ISPs (with 1,001 to 10,000 subscribers).[18] Additionally, there are a number of smaller ISPs that act as "virtual" providers, maintaining only a retail presence and offering end users access through the network facilities of other companies; these providers are carriage service providers and do not require a license.[19] Larger ISPs, which are referred to as carriers, own network infrastructure and are required to obtain a license from the Australian Communications and Media Authority (ACMA) and submit to dispute resolution by the Telecommunications Industry Ombudsman (TIO).[20] Australian ISPs are co-regulated under Schedule 7 of the 1992 Broadcasting Services Act (BSA), meaning there is a combination of regulation by the ACMA and self-regulation by the telecommunications industry.[21] The industry's involvement consists of developing industry standards and codes of practice.[22]

The ACMA is the primary regulator for the internet and mobile telephony.[23] Its oversight is generally viewed as fair and independent, though there are some transparency concerns with regard to the classification of content. Small businesses and residential customers may file complaints about internet, telephone, and mobile-phone services with the TIO,[24] which operates as a free and independent dispute-resolution service.

Limits on Content

Australian law does not currently provide for mandatory blocking or filtering of websites, blogs, chat rooms, or platforms for peer-to-peer file sharing. Access to online content is far-reaching, and Australians are able to explore all facets of political and societal discourse, including information about human rights violations. The ability to openly express dissatisfaction with politicians and to criticize government policies is not hindered by the authorities, and complaints may be sent directly

17 Telstra, page 19.

18 Australian Bureau of Statistics, "8153.0 – Internet Activity, Australia, December 2013: Type of Access Connection," accessed May 1, 2014, http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/8153.0Chapter5December%202013.

19 Australian Bureau of Statistics, "Internet Activity, Australia, Dec. 2009," http://www.abs.gov.au/AUSSTATS/abs@.nsf/0/58F65E39FB7E1064CA2577A10015467F?opendocument

20 Australia Communications and Media Authority, "Carriage & Service Provider Requirements, accessed March 2013, http://www.acma.gov.au/WEB/STANDARD..PC/pc=PC_1622.

21 Australian Communications and Media Authority Act 2005, http://www.austlii.edu.au/au/legis/cth/consol_act/acamaa2005453/;
Broadcasting Services Act 1992, http://www.austlii.edu.au/au/legis/cth/consol_act/bsa1992214/;
ACMA, "Service Provider Responsibilities," accessed June 2010, http://www.acma.gov.au/WEB/STANDARD/1001/pc=PC_90157.

22 Chris Connelly and David Vaile, "Drowning in Codes: An Analysis of Codes of Conduct Applying to Online Activity in Australia," Cyberspace Law and Policy Centre, March 2012, http://cyberlawcentre.org/onlinecodes/report.pdf.

23 ACMA, "The ACMA Overview," accessed March 2012, http://www.acma.gov.au/WEB/STANDARD/pc=ACMA_ORG_OVIEW;
ACMA, "About communications & media regulation," accessed March 2012, http://www.acma.gov.au/WEB/STANDARD/pc=PUB_REG_ABOUT.

24 Telecommunications Industry Ombudsman, accessed March 2012, http://www.tio.com.au.

to the Telecommunications Industry Ombudsman.[25] However, the legal guidelines and technical practices by which ISPs filter illegal material on websites have raised some concerns in the past years. Controversy struck in May 2013 when it was revealed that a number of legitimate Australian websites that did not host any type of illegal or even controversial material had been blocked. Investigations revealed that the Australian Security and Investment Commission was using an obscure provision (section 313) of the Telecommunications Act to request the blocking of a fraudulent website.[26] The notice by ASIC to the ISPs specified an IP address that contained the fraudulent website along with a number of legitimate websites, including that of Melbourne Free University. This is the first known incident of ASIC using section 313 to issue notices to ISPs to block non-Interpol material. While access to the affected websites was quickly restored, the use of section 313 in this matter was contentious.

It has meanwhile been reported in the news that the federal cabinet is considering two proposals that address piracy and the illegal downloading of content protected by intellectual property rights. The first proposal will require ISPs to issue warnings to users who repeatedly download illegal content (predominantly songs, movies, and TV shows) within a "graduated response scheme" where repeat offenders may have their internet accounts temporarily suspended.[27] The second proposal will force ISPs to block file-sharing sites such as Pirate Bay.[28] However, neither initiative has been formalized into a proposal or bill at this point.

As of May 2014, parliament is considering a bill that would allow automated classification tools to be used in lieu of or to aid the classification of publications, films, and computer games.[29] The bill is mainly procedural at this point. There is no information as to the type or nature of "classification tools" that would be used, or how they would change the workflow and human input into the classification process. In the bill's current wording, the minister of communications would have wide discretion to approve any tool. The bill has been criticized for not requiring transparency in the selection of classification tools, and for not having a sunset clause that would require reviewing the use of tools after a trial period.[30]

There are no examples of online content manipulation by the government or partisan interest groups. Journalists, commentators, and ordinary users have generally not been subject to censorship so long as their content does not amount to defamation or breach criminal laws, such as those against hate speech or racial vilification.[31] Nevertheless, the need to avoid defamation and, to a lesser extent, contempt of court has been a driver of self-censorship by both the media and ordinary

25 Ibid.

26 LeMay, R., "Interpol Filter Scope Creep: ASIC Ordering Unilateral Website Blocks," May, 15, 2013, accessed July 16, 2014, http://delimiter.com.au/2013/05/15/interpol-filter-scope-creep-asic-ordering-unilateral-website-blocks/

27 Hefferman, M., *Sydney Morning Herald*, "Online Piracy crackdown looms," May 5, 2014, http://www.smh.com.au/business/online-piracy-crackdown-looms-20140505-37r3g.html.

28 Knot, M., *Sydney Morning Herald*, "George Brandis signals internet filter rebirth," February 15, 2014, http://www.smh.com.au/it-pro/government-it/george-brandis-signals-internet-filter-rebirth-20140214-hvchm.html.

29 *Classification (Publications, Films and Computer Games) Amendment (Classification Tools and Other Measures) Bill 2014 (Cth)*.

30 Cyberspace Law and Policy Community, UNSW Law, Submission to Senate Legal and Constitutional Affairs Legislation Committee Inquiry into the Classification (Publications, Films and Computer Games) Amendment (Classification Tools and Other Measures) Bill 2014 (file on copy with the author, May 15, 2014).

31 *Jones v. Toben* [2002] FCA 1150 (17 September 2002), http://www.austlii.edu.au/au/cases/cth/FCA/2002/1150.html.

users (see "Violations of User Rights"). For example, narrowly-written suppression orders are often interpreted by the media in an overly broad fashion so as to avoid contempt of court charges.[32] There remains a lack of adequate legislative protection for the confidentiality of journalist's sources.[33] However, on a positive note, on January 15, 2014, the Commonwealth Public Interest Disclosure Act came into force providing protection to whistleblowers. Previously, whistleblowing protection was only for those disclosing information from State government initiatives; the protection now extends to the Commonwealth government.

Aside from the restrictions on prohibited content, including the incitement of violence, racial vilification, and defamation, Australians have access to a broad choice of online news sources that express diverse, uncensored political and social viewpoints. Individuals are able to use the internet and other technologies both as sources of information and as tools for mobilization. One interesting development has been the announcement by the new attorney general, George Brandis of his desire to repeal S 18C of the Racial Discrimination Act 1975 (Cth). Section 18C, otherwise known as the hate speech provision, currently makes it unlawful to commit an act (by any medium of communication) that is likely to offend, insult, humiliate or intimidate another party based on race, colour, or national or ethnic origin of another party. The announcement was met with strong public backlash from organizations and entities dedicated to combating racism online.[34] Ultimately the Abbott administration announced that it would not move forward with the proposal to remove section 18C of the legislation.[35]

Advanced web applications like the social-networking sites Facebook and MySpace, the Skype voice-communications system, and the video-sharing site YouTube are neither restricted nor blocked in Australia. Digital media such as blogs, Twitter feeds, Wikipedia pages, and Facebook groups have been harnessed for a wide variety of purposes ranging from elections to campaigns against government corporate activities, to a channel for safety-related alerts where urgent and immediate updates were required.[36]

Violations of User Rights

While online users in Australia are generally free to access and distribute materials online, free speech is limited by a number of legal obstacles, such as broadly applied defamation laws and a lack of codified free speech rights. Over the past year, revelations regarding global surveillance and retention of communications data by the NSA and other intelligence agencies have raised concerns regarding users' right to privacy and freedom of expression. However, the Australian government has

32 Nick Title, "Open Justice – Contempt of Court" (paper presentation, Media Law Conference Proceedings, Faculty of Law, The University of Melbourne, February 2013).

33 Jackson, S., *The Australian*, "Australia slips down press freedom rankings" February 12, 2014, http://www.theaustralian.com.au/media/australia-slips-down-press-freedom-rankings/story-e6frg996-1226824874302.

34 The Online Hate Prevention Institute "OHPI Submission on racial Discrimination and s18C," April 30, 2014, http://ohpi.org.au/ohpi-submission-on-racial-discrimination-and-s-18c/.

35 Heath Aston, "Tony Abbott dumps controversial changes to 18C racial discrimination laws," *The Sydney Morning Herald*, August 5, 2014, http://www.smh.com.au/federal-politics/political-news/tony-abbott-dumps-controversial-changes-to-18c-racial-discrimination-laws-20140805-3d65l.html.

36 Digital media, for example, is readily used for political campaigning and political protest in Australia. See Terry Flew, "Not Yet the Internet Election: Online Media, Political Content and the 2007 Australian Federal Election,"(2008) *Media International Australia Incorporating Culture and Policy*, pp. 5-13. Also available at http://eprints.qut.edu.au/39366/1/c39366.pdf

taken few steps to remedy these concerns, and in October 2014, the parliament passed amendments to the national security legislation that increase penalties for whistleblowers and could potentially allow intelligence agents to monitor an entire network with a single warrant.

Australians' rights to access internet content and freely engage in online discussions are based less in law and more in the shared understanding of a fair and free society. Legal protection for free speech is limited to the constitutionally-implied freedom of political communication, which only extends to the limited context of political discourse during an election.[37] There is no bill of rights or similar legislative instrument that protects the full range of human rights in Australia, and the courts have less ground to strike down legislation that infringes on civil liberties. Nonetheless, Australians benefit greatly from a culture of freedom of expression and freedom of information, further protected by an independent judiciary. The country is also a signatory to the International Covenant on Civil and Political Rights (ICCPR).

The Australian press, however, has consistently expressed concerns about a "culture of secrecy" that continues to inhibit reporting.[38] A 2007 report commissioned by Australia's Right to Know (ARTK), a coalition of media companies formed to examine free press issues, found that there were over 350 pieces of legislation containing "secrecy" provisions to restrict media publications.[39] As revealed in the Media Entertainment & Arts Alliance report on press freedom in Australia, secrecy and surveillance remain a critical issue.[40]

The Anti-Terrorism Act 2005 (Cth) revived laws against sedition and unlawful association. The unlawful association provisions have been used widely since their enactment to ban several organizations perceived to be potentially dangerous in terms of their links to violent acts.[41] The sedition provisions, however, have not been used. Further, insults against government institutions or officials would not fall within the sedition provisions.[42]

Australian defamation law has been interpreted liberally and is governed by legislation passed by the states as well as common law principles.[43] Civil actions over defamation are common and form the main impetus for self-censorship,[44] though a number of cases have established a constitutional defense when the publication of defamatory material involves political discussion.[45] Court costs and

37 Alana Maurushat, Renee Watt, "Australia's Internet Filtering Proposal in the International Context," *Internet Law Bulletin* 12, no. 2 (2009).

38 David Rolph, Matt Vitins, and Judith Bannister, *Media Law: Cases, Materials and Commentaries* (South Melbourne: Oxford University Press, 2010): 44. See also Irene Moss, *Report of the Independent Audit into the State of Free Speech in Australia* (Surry Hills, New South Wales: Australia's Right to Know Coalition, 2007), http://www.smh.com.au/pdf/foIreport5.pdf.. See also LexMedia Australia, "Journalist Shield Laws in Australia" (2010) http://www.lexmedia.com.au/2010/10/journalist-shield-laws.html#.UTfUOHnh2F8.

39 Australia's Right to Know, "Submission to the Australian Law Reforms Commission's Review of Secrecy Laws" (2007) http://www.australiasrighttoknow.com.au/files/docs/ALRC-Secrecy-Submission.pdf.

40 Federal Secretary Warren, C., Press Freedom – Secrecy and Surveillance: The report into the state of press freedom in Australia in 2014 "(2014), page 8, accessed May 8, 2014, http://www.pressfreedom.org.au/.

41 Andrew Lynch and George Williams, *What Price Security?* (UNSW Press: Sydney, 2006), 41-59.

42 Ibid.

43 Principles of online defamation stem from the High Court of Australia, *Dow Jones & Company Inc v. Joseph Gutnick*, [2002] HCA 56.

44 Moss, 42.

45 Human Rights Constitutional Rights, "Australian Defamation Law," http://www.hrcr.org/safrica/expression/defamation.html, accessed June 2010.

the stress associated with defending against suits under Australia's expansive defamation laws have caused organizations to leave the country and blogs to shut down.[46]

Under Australian law, a person may bring a defamation case to court based on information posted online by someone in another country, providing that the material is accessible in Australia and that the defamed person enjoys a reputation in Australia. In some cases, this law allows for the possibility of libel tourism, which allows individuals from any country to take up legal cases in Australia because of the more favorable legal environment regarding defamation suits. The right to reputation is generally afforded greater protection in countries like Australia and the United Kingdom than the right of freedom of expression. In Australia this is especially so as freedom of expression is limited to political speech. While the United States and the United Kingdom have recently enacted laws to restrict libel tourism, Australia is not currently considering any such legislation.

In the recent case of *Mickle v Farley*,[47] a young man in New South Wales was fined AUD 105,000 plus costs for posting defamatory statements on Twitter and Facebook about his music teacher. The student's father was also a teacher at the school. The father left his position due to health reasons but the student grudgingly blamed the new teacher, Ms. Mickle, who took his father's position. The comments greatly distressed Ms. Mickle, forcing her to take sick leave shortly after the allegedly hateful comments were posted to social media. The case is novel for the amount of damages incurred on the defendant and for being the first Australian decision where a tweet was held to be defamatory.[48] In the case Judge Elkaim stated that "when defamatory publications are made on social media it is common knowledge that they spread. They are spread easily by the simple manipulation of mobile phones and computer. Their evil lies in the grapevine effect that stems from the use of this type of communication."[49]

There have been several cases in the states of New South Wales and Victoria of individuals being sentenced to jail terms for publishing explicit photos of women, typically former girlfriends or boyfriends. By way of example, Australian citizen Ravshan Usmanov pled guilty to publishing an indecent article and was originally sentenced to six months of home detention after he posted nude photographs of an ex-girlfriend on Facebook.[50] The sentence was appealed and the court commuted the original sentence in favor of a suspended sentence.

Users do not need to register to use the internet, nor are there restrictions placed on anonymous communications. The same cannot be said of mobile phone users, as verified identification information is required to purchase any prepaid mobile service. Additional personal information must be provided to the service provider before a phone may be activated. All purchase information is stored while the service remains activated, and it may be accessed by law enforcement and emergency agencies provided there is a valid warrant.[51]

46 Asher Moses, "Online Forum Trolls Cost me Millions: Filmmaker," *Sydney Morning Herald*, July 15, 2009, http://www.smh.com.au/technology/technology-news/online-forum-trolls-cost-me-millions-filmmaker-20090715-dl4t.html.

47 *Mickle v Farley* [2013] NSWDC 295.

48 A 2011 case involving writer and TV personality Marieke Hardy reached a legal settlement in 2012.

49 Ibid. Line 21.

50 Heath Astor, "Ex-Lover Punished for Facebook Revenge," April 22, 2012, *Sydney Morning Herald*, http://www.smh.com.au/technology/technology-news/exlover-punished-for-facebook-revenge-20120421-1xdpy.html.

51 ACMA, "Pre-paid Mobile Services—Consumer Information Provision Fact Sheet," accessed June 2010, http://www.acma.gov.au/WEB/STANDARD/pc=PC_9079.

Law enforcement agencies may search and seize computers and compel an ISP to intercept and store data from those suspected of committing a crime. Such actions require a lawful warrant. The collection and monitoring of the content of a communication falls within the purview of the Telecommunications (Interception and Access) Act 1979 (TIAA). Call-charge records, however, are regulated by the Telecommunications Act 1997 (TA).[52] It is prohibited for ISPs and similar entities, acting on their own, to monitor and disclose the content of communications without the customer's consent.[53] Unlawful collection and disclosure of the content of a communication can draw both civil and criminal sanctions.[54] The TIAA and TA expressly authorize a range of disclosures, including to specified law enforcement and tax agencies, all of which require a warrant. ISPs are currently able to monitor their networks without a warrant for "network protection duties," such as curtailing malicious software and spam.[55]

On August 22, 2012, the Australian Senate passed the Cybercrime Legislation Amendment Bill, allowing Australia to accede to the Council of Europe Convention on Cybercrime.[56] Unlike the legislation of many other countries that have already ratified the convention, Australia's legislation goes beyond the treaty's terms by calling for greater monitoring of all internet communications by ISPs. Under the Convention, an ISP is only required to monitor, intercept, and retain data when presented with a warrant, and only in conjunction with an active and ongoing criminal investigation restricted to the areas in the Convention: child pornography, online copyright (intellectual property), online fraud and forgery, and computer offenses. The new Australian legislation compels ISP cooperation for any serious crime being investigated in Australia or overseas; it is not limited to the crimes set out in the Convention.

The Convention also requires expeditious preservation of data by the person in possession or control of data, which means ISPs will often be the ones called upon to store data. Articles 16 and 17 of the Convention state that ISPs can be compelled to preserve internet traffic data logs for a maximum period of 90 days, whereas the Australian legislation mandates that ISPs store data for 180 days for foreign preservation notices. However, the Convention does not compel ISPs to monitor stored communications, only traffic data. In the case of an active criminal investigation, the Convention obligates an ISP to preserve the data that is already stored but would otherwise be deleted. This could include preservation of what IP addresses connect to and from other IP addresses, or what phone numbers connect to a Voice over Internet Protocol (VoIP) number. This may also include information about what types of protocols a customer uses, the size and use of packets, and so forth. Data preservation remains a controversial point but most notably in relation to the obligation to provide mutual assistance to a foreign entity.

In July 2012, the Commonwealth Attorney-General's Department released a discussion paper titled

52 Telecommunications Act 1997, Part 13, http://www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/.

53 Part 2-1, section 7, of the Telecommunications (Interception and Access) Act 1979 (TIAA) prohibits disclosure of an interception or communications, and Part 3-1, section 108, of the TIAA prohibits access to stored communications. See Telecommunications (Interception and Access) Act 1979, http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/.

54 Criminal offenses are outlined in Part 2-9 of the TIAA, while civil remedies are outlined in Part 2-10. See Telecommunications (Interception and Access) Act 1979, http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/.

55 Alana Maurushat, "Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Obfuscation Crime Tools?" (2010) *University of New South Wales Law Journal* 16.1.

56 Council of Europe, Convention on Cybercrime, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG.

"Equipping Australia against emerging and evolving threats."[57] Under the proposal, Australian ISPs would be required to monitor, collect, and store information pertaining to all users' communications, including storing communications, for a period of two years. This activity would be done without a warrant and enforced against all users regardless of whether there is a criminal investigation.[58] The Attorney-General has failed to discuss the significant differences between the EU, American, and Australian legal environments. In other countries, citizens' rights are protected under a Bill of Rights or a Charter of Human Rights and Freedoms. Like the U.S. courts, European courts can strike down laws or directives that offend these guarantees of fundamental human rights and civil liberties. There is no Bill of Rights or Charter of Human Rights and Freedoms in Australia. As such, the courts have no effective means to strike down proposals that violate civil liberties. Once a proposal is enacted, the only way to have it changed is through legislation, which often requires a change of government. This compulsory data retention policy, if enacted, could become a significant threat to internet freedom in Australia. The proposal is not yet official policy in Australia, nor has it evolved to a bill. At this point in time it remains a proposal only.

Following the leaks of U.S. National Security Agency documents by former contractor Edward Snowden in June 2013, it was reported that Australian law enforcement has received information from the NSA surveillance programs. It is further believed that the attorney general's department is seeking the power to "break into anonymization and encryption software like Tor."[59]

The NSA surveillance revelations have further impacted the way in which Australia views its obligations around classified data. On October 1, 2014, the parliament enacted amendments to the National Security Legislation Amendment Act, including provisions that threaten journalists and whistleblowers with a ten year prison term if they publish classified information.[60] These provisions have already come into force. Other worrying provisions that will come into force in 2015 include changes to the scope of warrants. The definition of a "computer" has been broadened to allow law enforcement to access data to multiple computers connected to a network with a single warrant. Cyberattacks and hacking incidents remain a common and growing concern in Australia. Several universities sustained denial-of-service (DoS) attacks lasting close to a week, disrupting all facets of online university research, teaching, and administration. Private corporations such as those in the mining industry continue to be attacked on a regular basis. The overall rate of cyberattacks has remained steady over the past few years.

57 Commonwealth Attorney-General's Department's Discussion Paper, *Equipping Australia against emerging and evolving threats*, 2012, accessed February 1, 2013, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/additional/discussion%20paper.pdf.

58 Asher Moses, "Web Snooping Policy Shrouded in Secrecy," *The Age*, June 17, 2010, http://www.theage.com.au/technology/technology-news/web-snooping-policy-shrouded-in-secrecy-20100617-yi1u.html.

59 Bernard Keane, Crikey, "The Greatest Threat to our Rights is the Attonrey-General's Department," June 5, 2013, http://www.crikey.com.au/2013/06/05/the-greatest-threat-to-our-rights-is-the-attorney-generals-department/.

60 National Security Legislation Amendment Act (No. 1) 2014 No. 108, 2014