Freedom House

Australia

	2014	2015
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	12
TOTAL* (0-100)	**17**	**19**

* 0=most free, 100=least free

Population:	**23.5 million**
Internet Penetration 2014:	**85 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2015 Status:	**Free**

Key Developments: June 2014 – May 2015

- New revisions to the Defense Trade Controls Act, passed in April 2015, include restrictions on encryption software that could discourage internet users from taking advantage of such tools for their digital security (see **Surveillance, Privacy and Anonymity**)
- The National Security Legislation Amendment, passed in October 2014, expands the definition of "computer" to include an entire computer network, which lawyers argue could be misinterpreted to permit surveillance on wide swaths of the internet (see **Surveillance, Privacy and Anonymity**).
- According to the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015, which came into effect in April 2015, law enforcement and intelligence agencies will no longer require a warrant to access and review metadata, with an exception for the metadata associated with journalists or their sources (see **Surveillance, Privacy and Anonymity**).

Introduction

Australians have generally enjoyed affordable, high-quality access to the internet and other digital media, with access continuing to expand over the past few years with the rollout of the alternative National Broadband Network. However 2015 has been a pivotal year for change, with Australia's internet freedom declining slightly from previous years.

The Liberal government, formerly guided in the telecommunications field by Minister of Communications Malcom Turnbull (who became prime minister in September 2015), continues to embrace technology, showing commitment to open up data sets for research and to improve internet connectivity throughout Australia. Under Turnbull's guidance the government continued to roll out an alternative National Broadband Network (NBN), particularly in regional areas that have had poor internet services. The original NBN under the former Labour government was to lay copper cables throughout Australia. The alternative NBN involves a scaled down version using less expensive fiber to the node (FTTN) and was developed after much criticism of the cost and effectiveness of the original NBN plan.[1]

Recent legislative amendments, however, raised concerns about government surveillance and the potential implications for privacy and freedom of expression. In October 2014, the Australian 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. Further, data retention amendments passed in March 2015 require telecommunication companies to store customers' metadata for two years, allowing law enforcement and intelligence agencies to access that metadata without a warrant.[2]

Obstacles to Access

There are few impediments or obstacles to internet access in Australia. Services continue to improve in remote and rural areas throughout Australia with both the young and elderly embracing connectivity. The ICT sector is mature and competitive with Australians enjoying fair and high-quality internet connectivity.

Availability and Ease of Access

Australia had an internet penetration rate of approximately 85 percent as of December 2014, compared to 83 percent in 2013 and 74 percent in 2009, according to the International Telecommunication Union (ITU).[3] The internet penetration rate is expected to steadily increase over the next five years with the implementation of the NBN, which includes expanded wireless, fiber to the node, and satellite services in rural communities. Although internet access is widely available in locations such

1 Australian Government, Department of Communications, *NBN Market and Regulation Report*, October 1, 2014, accessed June 4, 2015 http://bit.ly/1VrlDDa. Also known as the "Vertigan Report".

2 For a comprehensive overview of the legislative history of censorship in Australia see Libertus, "Australia's Internet Censorship System," accessed February 12, 2015, http://bit.ly/1JCpGpq; See also Australian Privacy Foundation, accessed February 12, 2015, http://www.privacy.org.au.

3 International Telecommunication Union, "Percentage of Individuals Using the Internet," 2009, 2013, 2014, http://bit.ly/1cblxxY.

as libraries, educational institutions, and cybercafes, 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+, mobile, fixed wireless, cable, satellite, fiber and dial-up.[5] Wireless systems reach 99 percent of the population, while satellite capabilities are able to reach 100 percent.[6] As of December 2014, over 99 percent of internet connections were broadband, while the number of dial-up connections has declined to 159,000 users out of a total of 12.7 million users.[7] Once implemented, the NBN is expected to 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 between 8 Mbps and 24 Mbps.[9] While there are still parts of Australia experiencing slower broadband speeds (approximately 3.3 million people have internet connection speeds of only 1.5 Mbps to 8 Mbps), there has been a steady increase in faster speeds with 2.3 million people connecting to speeds of greater than 24 Mbps.[10] According to Akamai, the average connection speed by the end of 2014 was 7.4 Mbps.[11]

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.[12] 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.[13] Of those with internet access, 85 percent access the internet through broadband connections.[14] The overall mobile phone penetration rate in Aboriginal communities is unknown.

According to the ITU, there were 31 million mobile phone subscribers in Australia by the end of 2014, compared to 25 million the previous year.[15] Fourth generation (4G) mobile services have driven recent growth, with all networks expanding coverage and experiencing increases in the number of services in operation.[16]

Internet access is affordable for most Australians even though the government no longer subsidizes internet connections for individuals and small businesses in remote and rural areas, where internet affordability is not comparable to that in metropolitan areas.[17] Major internet service providers (ISPs)

4 Australian Bureau of Statistics (ABS), "8146.0 - Household Use of Information Technology, Australia, 2012-13: Personal internet use," February 25, 2014, http://bit.ly/1dmbJ5W.

5 ABS, "8153.0 – Internet Activity, Australia, December 2014: Type of Access Connection," April 1, 2015, accessed June 18, 2015, http://bit.ly/1L4e9Vh.

6 ABS, "8153.0 – Internet Activity, Australia, December 2013: Type of Access Connection," April 8, 2014, http://bit.ly/1QLazj3.

7 ABS, "8153.0 – Internet Activity, Australia, December 2014: Type of Access Connection."

8 NBNCo, "NBN set to narrow digital divide for 400,000 homes and businesses," media release, February 09, 2015, http://bit.ly/16VvWwI.

9 ABS, "8153.0 – Internet Activity, Australia, December 2014: Type of Access Connection: Advertsied Download Speed."

10 ABS, "8153.0 – Internet Activity, Australia, December 2014: Type of Access Connection: Advertsied Download Speed."

11 Akamai, Stae of the Internet: Q4 2014 Report, http://bit.ly/1LpozZz.

12 ABS, "8146.0 - Household Use of Information Technology, Australia, 2012-13: Personal internet use."

13 ABS, "Census of Population and Housing: Characteristics of Aboriginal and Torres Strait Islander Australians, 2011," November 27, 2012, accessed June 18, 2015, http://bit.ly/1FIldX3.

14 ABS, "Census of Population and Housing: Characteristics of Aboriginal and Torres Strait Islander Australians, 2011."

15 International Telecommunication Union, "Mobile-cellular telephone subscriptions," 2014, http://bit.ly/1cblxxY.

16 Australian Communications and Media Authority (ACMA), *Communications Report, 2013-14* (Canberra: ACMA, 2013) 8 and 18, http://bit.ly/1DlBmjB.

17 Australian Government, Department of Communications, "Satellite Phone Subsidy Scheme," February 27, 2014, accessed

such as Telstra also continue to offer financial assistance for internet connections to low-income families.[18]

Restrictions on Connectivity

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 user, the internet connectivity for those activities will be slowed down to free bandwidth for other applications.[19] Under the iCode, a set of voluntary guidelines for ISPs related to cybersecurity, internet users whose devices have become part of a botnet or who are at high risk of their devices being infected with malware may have their internet service temporarily throttled, or placed in a temporary wall-garden after notification.[20] The ISP supplies the user with information and helps them to clean their devices to become free from botnets and malware. While the aim of the iCode is to improve cybersecurity, in its operation internet connectivity may become temporarily restricted.

ICT Market

Like most other industrialized nations, Australia hosts a competitive market for internet access, with 71 providers as of December 2014, nine of which are very large ISPs (over 100,000 subscribers), another 21 large ISPs (with 10,001 to 100,000 subscribers), and 41 medium ISPs (with 1,001 to 10,000 subscribers).[21] 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.[22] 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).[23] 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.[24] The industry's involvement consists of developing industry standards and codes of practice.[25]

June 18, 2015, http://bit.ly/1PNLtzM.

18 Telstra, *Bigger Picture 2014 Sustainability Report*, accessed February 13, 2015, 6-7, http://bit.ly/1FIlNUM.

19 Telstra, *Telstra Sustainability Report 2011*, (Sydney, Australia: 2011) accessed February 13, 2015, 19, http://bit.ly/1haWjDQ.

20 *Industry Code C650:2014 iCode: Internet Service Providers Voluntary Code of Practice for Industry Self-Regulation in the Area of Cybersecurity,* (Australia, Communications Alliance, LTD: 2010) accessed June 4, 2015, http://bit.ly/1GhwCIm.

21 ABS, "8153.0 – Internet Activity, Australia, December 2014: Number of Internet Service Providers (ISPs)," April 1, 2015, accessed June 18, 2015, http://bit.ly/1GhwZ5U.

22 ABS, "Internet Activity, Australia, Dec. 2009," March 30, 2010, http://bit.ly/1VnetVV.

23 ACMA, "Carrier & Service Provider Requirements, August 2, 2012, http://bit.ly/1QLdckO.

24 *Australian Communications and Media Authority Act* 2005, accessed February 2, 2015, http://bit.ly/1jz1CyZ; *Broadcasting Services Act* 1992, accessed February 2, 2015, http://bit.ly/1VneSrn; ACMA, "Service Provider Responsibilities," November 27, 2012, http://bit.ly/1FEL6ri.

25 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, Sydney, March 2012, http://bit.ly/1Vnfj54.

Regulatory Bodies

The ACMA is the primary regulator for the internet and mobile telephony.[26] Its oversight is generally viewed as fair and independent, though there are some transparency concerns with regard to the classification of content. The ACMA approves self-regulatory "codes" negotiated among members of the Internet Industry Association (IIA). There are over 30 self-regulatory codes that govern and regulate Australian ICTs. In March 2014 the Communications Alliance took over the responsibilities of the IIA through a signed agreement.[27]

Small businesses and residential customers may file complaints about internet, telephone, and mobile-phone services with the TIO,[28] which operates as a free and independent dispute-resolution service.

Limits on Content

There are relatively few limits to online content. However, at times those limits have been the source of controversy for their potential impediment to online freedoms and privacy, such as cases where the attempt to block illegal content online led to the blocking of legitimate content as well.

Blocking and Filtering

Australian law currently does not provide for mandatory blocking or filtering of blogs, chat rooms, or platforms for peer-to-peer file sharing. Websites are blocked or filtered under a narrow set of restrictions. 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 to the TIO.[29] 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.[30] 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. This led to a formal review of section 313(3) in 2015 to

26 ACMA, "The ACMA Overview," August 20, 2012, http://bit.ly/1jz2hQL; ACMA, "About communications & media regulation," August 20, 2012, http://bit.ly/1OGxfn0.

27 Communications Alliance, "Internet Service Provider Industry," August 19, 2014, accessed June 4, 2015, http://bit.ly/1LptIRq.

28 Telecommunications Industry Ombudsman, accessed February 13, 2015, http://www.tio.com.au.

29 Telecommunications Industry Ombudsman.

30 Renai LeMay, "Interpol filter scope creep: ASIC ordering unilateral website blocks," *Delimiter*, May 15, 2013, http://bit.ly/1OGxYoc.

investigate public policy concerns.[31] The committee's final report was released on June 1, 2015 but has not yet resulted in any new bills or amendments to section 313(3) of the Telecommunications Act.[32]

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.[33]

While the government does not block social media applications within the country, there were some reports in May 2015 that alleged that the Australian government made an informal request for the government of Nauru to block Facebook on the island, though these reports remain unconfirmed. Advocates suspected the Australian government's involvement due to the fact that Nauru hosts one of Australia's offshore processing centers for asylum seekers and refugees, and blocking Facebook in Nauru limits refugees in their ability to contact family in Australia. It was reported that the request was made to assist in the Cambodian resettlement policy.[34] UN Special Rapporteur on Freedom of Expression David Kaye also urged the government to revoke the blocking, expressing concern that the measure was "designed to prevent asylum seekers and refugees in the country from sharing information on their situation."[35]

In March 2015, the Communications Alliance developed the Industry Code Copyright Infringement Scheme, which would require ISPs to issue warnings to users who repeatedly download content illegally (predominantly songs, movies, and TV shows) within a "graduated response scheme" (GRS) where offenders will be warned of their illegal online activity.[36] Unlike GRS systems in other countries such as France and New Zealand, the Australian Scheme does not allow an ISP to terminate an account, apply fines, or throttle those whose activities infringe copyright. As of June 2015, this scheme has not yet been enacted. The Copyright Amendment (Online Infringement) Bill (No 44) 2015, which was passed in June 2015 (outside of this report's coverage period) will force ISPs to block file-sharing sites such as The Pirate Bay.[37] The bill allows a copyright owner to apply to the Federal Court to order an ISP to block access to a website whose primary purpose is copyright infringement for sites located outside of Australia.[38] It remains uncertain if these measures will be effective, or even enforced.

31 Parliament of Australia, "Inquiry into the use of subsection 313(3) of the Telecommunications Act 1997 by Government Agencies to Disrupt the Operations of Online Legal Services," accessed June 1, 2015, http://bit.ly/1zQYodS.

32 House Of Representatives Standing Committee of Infrastructure and Communications, *Balancing Freedom and Protection*, June 1, 2015) http://bit.ly/1RgfhWT.

33 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," *Media International Australia Incorporating Culture and Policy*, no. 126, (2008) 5-13, http://eprints.qut.edu.au/39366/1/c39366.pdf.

34 Suzie Raines, "Nauru Facebook Ban Came 'at request of Australian Government', Refugee Advocates Say" *ABC*, May 4, 2015, accessed June 4, 2015, http://ab.co/1PihLBl.

35 David Kaye, "UN rights expert urges Nauru to withdraw norms threatening freedom of expression, May 22, 2015, UN OHCHR, accessed September 1, 2015, http://bit.ly/1QLgMv6.

36 Madeleine Hefferman, "Online Piracy crackdown looms," *Sydney Morning Herald*, May 5, 2014, http://bit.ly/1MGFwUB.

37 Matthew Knot, "George Brandis signals internet filter rebirth," *Sydney Morning Herald*, February 15, 2014, http://bit.ly/MQXJ7J.

38 House of Representatives, Copyright Amendment (Online Infringement) Bill 2015, accessed June 18, 2015, http://bit.ly/1zEHKM6.

Content Removal

There were no cases of the government or other parties forcing content to be removed from websites during the coverage period.

Media, Diversity, and Content Manipulation

The online landscape in Australia is fairly diverse, with content available on a wide array of topics. There are no examples of online content manipulation by the government or partisan interest groups. Journalists, commentators, and ordinary internet 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.[39] 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 users. 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.[40]

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 as sources of information. Additionally, publicly funded television station SBS features first-rate news programs in multiples languages (available offline and online) to reflect the cultural diversity found in the Australian population.

Digital Activism

Australians use social media to sign petitions to the government, share controversial information, and to mobilize for public protest. Popular protests in 2015 included rallying against the closure of Aboriginal communities in Western Australia,[41] protests against Halal meat[42] and protests at the G20 Summit in Brisbane.[43]

Violations of User Rights

While internet 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. Additionally, recent amendments have significantly increased the government's capacity for surveillance of ICTs, including an amendment broadening the definition of "computer" to include entire networks, and a provision allowing law enforcement and intelligence agencies warrantless access to metadata.

39 *Jones v. Toben (2002) FCA 1150, September 17, 2002,* http://bit.ly/1KSeqX0.

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

41 Sarah Tallier, "Rallies held to protest against threat of remote community closures in Western Australia," *ABC*, May 1, 2015, accessed June 18, 2015, http://ab.co/1YOVQJK.

42 John Elder, "So this Easter: Melbourne faces off at anti-Islam rally as police on horseback hold factions apart," *The Age*, April 5, 2015, accessed June 18, 2015, http://bit.ly/1O8ghOo.

43 Occupy G20 Brisbane, Facebook Community Page, accessed June 18, 2015, http://on.fb.me/1j12qN2.

Legal Environment

Australians' rights to access online 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.[44] 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).

Australian defamation law has been interpreted liberally and is governed by legislation passed by the states as well as common law principles.[45] Civil actions over defamation are common and form the main impetus for self-censorship, though a number of cases have established a constitutional defense when the publication of defamatory material involves political discussion.[46] Court costs and 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.[47]

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.

Prosecutions and Detentions for Online Activities

In January 2015, a Western Australian court ordered estranged wife Robyn Greeuw to pay $12,500 in damages for her defamatory Facebook postings where she alleged that her former husband Miro Dabrowski had emotionally and physically abused her for over 18 years.[48] The defence of truth was not proven. This follows the widely publicized earlier decision in the case of *Mickle v Farley*,[49] where 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 case was novel for the amount of damages incurred on the defendant and for being the first Australian decision where a tweet was held to

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

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

46 Human Rights Constitutional Rights, "Australian Defamation Law," accessed February 13, 2015, http://bit.ly/1GhEp9a.

47 Asher Moses, "Online forum trolls cost me millions: filmmaker," *Sydney Morning Herald*, July 15, 2009, http://bit.ly/1VrnCY8.

48 Calla Wahlquist, "Facebook defamation: man wins lawsuit over estranged wife's domestic violence post", *The* Guardian, January 2, 2015, accessed June 4, 2015, http://gu.com/p/44hax/stw.

49 *Mickle v Farley* (2013) NSWDC, 295.

be defamatory.[50] 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."[51]

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, in 2012 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.[52] The sentence was appealed and the court commuted the original sentence in favor of a suspended sentence.

Surveillance, Privacy, and Anonymity

Over the past few years, 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 taken few steps to remedy these concerns, and has instead moved to expand the government's surveillance capabilities. 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. Further, data retention amendments passed in March 2015 require telecommunication companies to store customers' metadata for two years, allowing agencies to access that metadata without a warrant.

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. As will be discussed below, law enforcement no longer requires a warrant to access, review, and store metadata. The collection and monitoring of the content of 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).[53] 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.[54] Unlawful collection and disclosure of the content of a communication can draw both civil and criminal sanctions.[55] The TIAA and TA explicitly 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.[56]

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

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

52 Heath Astor, "Ex-Lover Punished for Facebook Revenge," *Sydney Morning Herald*, April 22, 2012, http://bit.ly/1N0J70Z.

53 Telecommunications Act 1997, part 13, accessed February 13, 2015, http://www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/.

54 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,part 2-1 s 7, part 3-1 s 108, accessed February 13, 2015, http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/.

55 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*, part 2-9 and part 2-10, accessed February 13, 2015, http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/.

56 Alana Maurushat, "Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Obfuscation Crime Tools?" *University of New South Wales Law Journal* 16, no. 1 (2010).

The *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 (Bill)* is potentially the greatest legislative threat to Australian online freedom. The bill amends the TIAA and TA while introducing a statutory obligation for telecommunication service providers to retain telecommunications data (metadata) for two years. The bill became law on April 13, 2015 and is now referred to as the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (the Act). Telecommunications providers have an 18 month grace period before the applicable provisions enter into force. The metadata of all Australians will be stored for two years. There is no longer the requirement of restricting metadata access and use only in the course of an investigation. Law enforcement and intelligence agencies will no longer require a warrant to access and review metadata. However, law enforcement will still need a warrant to access stored communications, as well as any metadata associated with journalists or their sources.

While other countries have implemented data retention frameworks, the Australian 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 and have struck down data retention 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.

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."[57]

Additionally, in April 2015, new revisions to the Defense Trade Controls Act introduced restrictions on encryption software that could discourage the use of these tools. The new revisions have been criticized for being overly broad, with the potential to criminalize the use of encryption for teaching and research purposes, in addition to everyday use for privacy and security.[58]

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.[59] These provisions have entered 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.

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

57 Bernard Keane, Crikey, "The Greatest Threat to our Rights is the Attorney-General's Department," Crickey, June 5, 2013, http://bit.ly/1KShz95.

58 Sarah Myers West, "The Crypto Wars Have Gone Global," *Deeplinks Blog,* Electronic Frontier Foundation, July 28, 2015, http://bit.ly/1MTHdxk.

59 *National Security Legislation Amendment Act* (No. 1) 2014, s 108.

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.[60]

Intimidation and Violence

There were no reported acts of intimidation or violence resulting from online activities during the reporting period.

Technical Attacks

Cyberattacks and hacking incidents remain a common concern in Australia. Several businesses and 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.

60 ACMA, "Pre-paid Mobile Services—Consumer Information Provision Fact Sheet," October 23, 2012, http://bit.ly/1KShSkd.