FREEDOM ON THE NET 2016

Australia

FREE

79 /100

A. Obstacles to Access	23 /25
B. Limits on Content	29 /35
C. Violations of User Rights	27 /40

Scores are based on a scale of 0 (least free) to 100 (most free)

Key Developments

- A new section of the Copyright Act passed in June 2015 would allow a copyright owner to apply to the Federal Court to compel an ISP to block access to an overseas website or service whose primary purpose is to facilitate copyright infringement (see Blocking and Filtering).
- A court found Google to be liable as a secondary publisher in an internet defamation case for failure to remove defamatory content from its search results, including content from its "autocomplete" function (see Content Removal).
- The Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 came into effect in October 2015, requiring telecommunications companies to retain metadata on their customers for two years. Law enforcement and intelligence agencies do not need a warrant to access and review metadata, except for metadata associated with journalists or their sources (see Surveillance, Privacy and Anonymity).
- A review of the controversial section 35P of the Security Intelligence Organisation Act recommended adding safeguards for journalists and sources who publish information about a special intelligence operation, but a bill to amend it has not yet materialized (see Surveillance, Privacy and Anonymity).

Introduction

Legislative developments on government surveillance and its potential implications for privacy and freedom of expression have led to a slight decline in internet freedom in Australia.

Australians have generally enjoyed affordable, high-quality access to the internet and other digital media as access has continued to expand over the past few years with the rollout of the alternative National Broadband Network.

The Liberal government, led by the former Minister of Communications Malcom Turnbull, has demonstrated a commitment to open data for research and to improving 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. While the original plan under the former Labor government was to lay copper cables throughout Australia, the alternative NBN opted for less expensive fiber to the node (FTTN) cables after much criticism of the cost and effectiveness of the original NBN plan. [1]

A new Federal election was held on July 2, 2016 with no parties winning the required 76 seats to form a majority government, resulting in the formation of a coalition government with three independent Members of Parliament supporting Prime Minister Malcom Turnbull's liberal government. Unlike in previous years, the NBN and internet blocking and filtering were not election issues. The newly formed government is not likely to introduce controversial amendments that would lead to further divisions within the party and between parties.

However, recent legislative amendments have significantly increased the government's capacity for surveillance of ICTs. Data retention amendments, which were passed in March 2015 and came into effect in October 2015, require telecommunication companies to store customers' metadata for two years and allows law enforcement and intelligence agencies to access that metadata without a warrant. [2] Moreover, despite calls to amend the Australian Security Intelligence Organisation (ASIO) Act, which includes provisions that threaten journalists and whistleblowers with a ten year prison term if they publish classified information in relation to special intelligence operations, no formal bills have been introduced to date to amend the controversial provision.

A. Obstacles to Access

There are few 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, providing Australians with fair and high-quality internet connectivity.

Availability and Ease of Access

Australia had an internet penetration rate of approximately 84.5 percent as of December 2015, 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 as libraries, educational institutions, and cybercafés, 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] As of June 2016, almost all of internet connections were broadband, while the number of dial-up connections declined to 90,000 users out of a total of 13.3 million users. [6] 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. [7]

Roughly 80 percent of all Australians have access to broadband speeds over 8 Mbps. [8] There are still parts of Australia experiencing slower broadband speeds (approximately 2.3 million people have internet connection speeds of only 1.5 Mbps to 8 Mbps). [9] According to Akamai, the average connection speed by the first quarter of 2016 was 8.8 Mbps. [10]

Age is a significant indicator of internet use: 99 percent of Australians between the ages of 15 and 17 are internet users, compared to only 51 percent of those over 65 years old. [11] 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. [12]

November 27, 2012, accessed February 5, 2016, http://bit.ly/1FIldX3. The overall mobile phone penetration rate in Aboriginal communities is unknown.

According to the ITU, there were 31.7 million mobile phone subscribers in Australia by the end of 2015, compared to 31 million the previous year. [13] Fourth generation (4G) mobile services have driven recent growth, with all networks expanding coverage and experiencing increases in the number of services in operation. [14]

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. [15] Major internet service providers (ISPs) such as Telstra continue to offer financial assistance for internet connections to low-income families. [16]

Restrictions on Connectivity

The government does not impose restrictions on connectivity to the internet or mobile networks in Australia.

There are no limits to the amount of bandwidth that ISPs can supply, though 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, internet connectivity for those activities will be slowed down to free bandwidth for other applications. [17]

Under the iCode, a set of voluntary guidelines for ISPs related to cybersecurity, internet connectivity may become temporarily restricted for internet users whose devices have become part of a botnet or who are at high risk of their devices being infected with malware. Such users may have their internet service temporarily throttled or placed in a temporary wall-garden after notification. [18] The ISP then supplies the user with information and helps them to clean their devices to become free from botnets and malware.

ICT Market

Australia hosts a competitive market for internet access, with 62 providers as of December 2015, ten of which are very large ISPs (over 100,000 subscribers), another

21 large ISPs (with 10,001 to 100,000 subscribers), and 31 medium ISPs (with 1,001 to 10,000 subscribers). [19]

http://bit.ly/2dDFo1p. 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. [20] 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). [21] Australian ISPs are co-regulated under Schedule 7 of the 1992 Broadcasting Services Act (BSA), which combines regulation by the ACMA with self-regulation by the telecommunications industry. [22] The industry's involvement consists of developing industry standards and codes of practice. [23]

Cyberspace Law and Policy Centre, Sydney, March 2012, http://bit.ly/1Vnfj54.

Regulatory Bodies

The Australian Communications and Media Authority (ACMA) is the primary regulator for the internet and mobile telephony. [24]

August 20, 2012, http://bit.ly/1OGxfno. 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. [25]

Small businesses and residential customers may file complaints about internet, telephone, and mobile phone services with the Telecommunications Industry Ombudsman (TIO), [26] which operates as a free and independent dispute-resolution service.

B. Limits on Content

There are relatively few limits to online content in Australia. However, the collateral blocking of legitimate content while targeting illegal content has harmed internet freedom in the past.

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. Web applications like the social-networking site Facebook, the Skype voice-communications system, and the video-sharing site YouTube are neither restricted nor blocked in Australia. 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 (ASIC) was using an obscure provision (section 313) of the Telecommunications Act to request the blocking of a fraudulent website. [27] ASIC's notice 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 was 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 investigate public policy concerns. [28] 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) or 314 of the Telecommunications Act. [29]

As of June 2015, copyright holders may now apply to the Federal Court to request that overseas copyright infringing locations (websites and services) be blocked by Australian ISPs under the newly amended section 115A of the Copyright Amendment (Online Infringement) Act 2015. [30] When making a decision, the court must take into

consideration whether the overseas online location has a primary purpose of facilitating copyright infringement, whether the response is proportionate in the circumstances, and whether or not blocking is in the public interest. [31] It is yet to be seen how the courts will interpret "primary purpose" and "blocking in the public interest" as to whether blocking could extend to websites that are mostly non-infringing.

In March 2015, the Communications Alliance also 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) warning offenders of their illegal online activity. [32] 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 the connections of users who infringe copyright. The scheme has not yet been implemented as it was deemed to be too expensive for copyright holders and ISPs to implement at present, but it may still be implemented in the future. [33]

Content Removal

There were no cases of the government forcing content to be removed from websites during the coverage period. However, a decision by the Supreme Court of South Australia in October 2015 found that Google was liable, as a secondary publisher, for defamatory content revealed in Google's search results, including results through the autocomplete function, snippets and hyperlinks to defamatory content published by third party websites against the plaintiff. [34] Google was ordered to pay damages to the plaintiff. [35] Reactions to the decision were mixed, although some commentators raised concerns that it could set a dangerous precedent for potential abuse by certain claimants seeking to censor legitimate criticism online. [36]

Media, Diversity, and Content Manipulation

The online landscape in Australia is fairly diverse, with content available on a wide array of topics. Australians have access to a broad choice of online news sources that

express diverse, uncensored political and social viewpoints. 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. [37] 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.

There are no examples of online content manipulation by the government or partisan interest groups. Journalists, commentators, and ordinary internet users generally do not face censorship, so long as their speech does not amount to defamation or breach criminal laws, such as those against hate speech or racial vilification (see Legal Environment). [38] Nevertheless, the need to avoid defamation (and, to a lesser extent, contempt of court) has been a driver of some 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. [39] 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. [40]

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]

C. 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, legislative amendments have significantly increased the government's capacity for surveillance

of ICTs, including a provision allowing law enforcement and intelligence agencies warrantless access to metadata.

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**

12, no. 2 (2009). 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**

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. Freedom of expression is not explicitly protected under constitutional or statutory rights, although the High Court has held that there is implied freedom of political communication in the constitution.

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

A number of lawsuits for defamation online have made the headlines in recent years. In a November 2015 trial, a jury found that a barrister had defamed a policeman, Sergeant Colin Dods, who was involved in the death of an armed teen, through comments he posted on a website in 2012. The incident in question occurred in December 2008, when teenager Tyler Cassidy entered a shopping mall yielding knives and advanced toward police officers, ignoring their requests to drop his weapons. [47] He was shot twice in the legs by Sergeant Dods, but when he continued to advance, he was shot dead. Some public outcry ensued, despite the coroner's findings that Dods' shots did not contribute to Cassidy's death and that the young man was shot dead after police officers were at risk of serious injury. The incident prompted a Queensland barrister, Mr. Michael McDonald, to publish a series of comments online calling for justice for Cassidy, accusing Dods of responsibility for Cassidy's death, proclaiming that Dods' shots were fired without provocation, and asserting that Cassidy's shooting was manslaughter. [48] The jury found that McDonald's statements were indeed defamatory, leading Justice Bell to award Dods aggravated damages totaling AUD $150,000 (approximately USD $114,000) due to the level of harm caused by the online publications. [49]

In an earlier case in January 2015, a Western Australian court ordered estranged wife Robyn Greeuw to pay AUD $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. [50] The defense of truth was not proven. This follows the widely publicized earlier decision in the case of *Mickle v Farley* from 2013, [51] 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 be defamatory. [52] 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." [53]

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, known as "revenge porn." 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. [54] 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 U.S. National Security Agency (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.

Law enforcement agencies may search and seize computers and compel an ISP to intercept and store data from those suspected of committing a crime with a lawful warrant, as governed by the Telecommunications (Interception and Access) Act 1979 (TIAA). Call-charge records are regulated by the Telecommunications Act 1997 (TA). [55] 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. [56] Unlawful collection and disclosure of the content of a communication can draw both civil and criminal sanctions. [57] 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. [58]

In a troubling development, law enforcement agencies no longer require a warrant to access, review, and store metadata under the Telecommunications (Interception and Access) Amendment (Data Retention) Act, which was passed in March 2015 and came into effect on October 13, 2015. The act requires telecommunication companies store customers' metadata for two years, which law enforcement and intelligence agencies can access and review without a warrant at any point, not just in the course of an investigation as was previously required. However, law enforcement still needs a warrant to access stored communications, as well as any metadata associated with journalists or their sources.

During this report's coverage period, a disturbing incident emerged regarding potentially inappropriate access and use of journalists' metadata. In February 2016, investigative journalist Paul Farrell of *The Guardian Australia* discovered that the Australian Federal Police (AFP) had looked at the metadata of his devices without a warrant, in what was thought to be an attempt to identify a source from an asylum seeker story. [59] In writing about the incident, Farrell stated that "over the years, under both Labor and Coalition governments, sensitive stories by journalists that embarrassed or shamed governments have often been referred to the AFP... However, this is the first time the AFP has ever made such an admission in Australia. They've acknowledged generally that they made requests for journalists' metadata in the past – and said they were rare – but never in a specific case." [60] The AFP argued that its investigations were not targeting journalists, but rather addressed breaches under Section 70 of the Crimes Act, notably "the offence relates to a Commonwealth officer disclosing Commonwealth information without authorization." [61] The AFP also told *The Guardian* that it "ha[d] not accessed or applied to access the metadata information belonging to any journalist since 13 October 2015" – which is when the Telecommunications (Interception and Access) Amendment (Data Retention) Act came into effect. [62]

In October 2014, parliament enacted amendments to national security legislation that increased penalties for whistleblowers and potentially allows intelligence agents to monitor an entire network with a single warrant. In particular, a new section (35P) was added to the Australian Security Intelligence Organisation Act 1979, which includes provisions that threaten journalists and whistleblowers with a ten-year

prison term if they publish classified information in relation to special intelligence operations. [63] The controversial amendment prompted a review by the independent national security legislation monitor, Robert Gyles QC, in October 2015 to specifically assess the impact of section 35P on journalists. Gyles' report concluded that section 35P was arguably invalid as it infringed on the constitutionally protected right of freedom of political communications and was inconsistent with article 19 of the International Covenant on Civil and Political Rights. [64] The government announced their intention to support the six recommendations included in Gyle's report to better protect journalists and their sources; however, no changes to section 35P have materialized to date. [65] Other worrying amendments to the Australian Security Intelligence Organisation Act include changes to the scope of warrants: notably, the definition of a "computer" was broadened to allow law enforcement to access data on multiple computers connected to a network with a single warrant.

In the midst of renewed debate over encryption, the right to privacy, and law enforcement in February 2016, both the Labor party and the Coalition voted against a Senate motion to support strong encryption. Meanwhile, April 2015 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. [66]

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. [67]

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. According to the Australian Cyber Security Centre (ACSC), the number of cyberattacks in Australia has increased since 2014, particularly on businesses and non-government agencies, with CERT Australia responding to over 11,000 cyberattacks in 2014 and over 800 confirmed instances on attacks to critical infrastructure, though the number of significant compromises of Australian Government networks has decreased. [68] Updated ACSC statistics for 2015 and 2016 are not available

Meanwhile, a 2015 Cyber Security Study showed that over 90 percent of Australian businesses had adopted at least three out of the four recommended Top 4 Strategies to Mitigate Targeted Cyber Intrusions. [69] While there are no metrics to ascertain whether significant compromises to business networks have decreased, there is a strong likelihood that this would be the case.

Footnotes

1. Australian Government, Department of Communications, NBN Market and Regulation Report, October 1, 2014, accessed June 4, 2015 http://bit.ly/1VrlDDa.
2. For a comprehensive overview of the legislative history of censorship in Australia see Libertus, "Australia's Internet Censorship System," accessed February 5, 2016, http://bit.ly/1JCpGpq; See also Australian Privacy Foundation, accessed February 5, 2016, http://www.privacy.org.au.
3. International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," accessed October 9, 2016, http://bit.ly/1cblxxY.
4. Australian Bureau of Statistics (ABS), "8146.0 - Household Use of Information Technology, Australia, 2014-2015: Personal internet use," February 18, 2016, http://bit.ly/1Ny07ND.
5. ABS, "8153.0 – Internet Activity, Australia, June 2016: Type of Access Connection," http://bit.ly/1Mq30uD.

More footnotes

On Australia

See all data, scores & information on this country or territory.

See More >

Country Facts

Global Freedom Score

97 /100 **Free**

Internet Freedom Score

76 /100 **Free**

Other Years

2020

Be the first to know what's happening.

Email

Subscribe

Join the Freedom House monthly newsletter

ADDRESS

1850 M St. NW Floor 11
Washington, DC 20036
(202) 296-5101

GENERAL INQUIRIES
info@freedomhouse.org

PRESS & MEDIA
press@freedomhouse.org

@2020 FreedomHouse