



## FREEDOM ON THE NET 2017

# Australia

# 79

/100

FREE

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

## LAST YEAR'S SCORE &amp; STATUS

79/100 Free

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



# Key Developments, June 1, 2016 - May 31, 2017

- As of 2017, telecommunication and internet providers must be compliant with recent data retention requirements. The government clarified that stored metadata cannot be used in civil court cases (see Surveillance, Privacy, and Anonymity).
- The Australian Federal Police accidentally accessed a journalist's metadata without authorization in April 2017, though the law requires them to seek a warrant (see Surveillance, Privacy, and Anonymity).
- Social media was an important platform for debate ahead of a nationwide survey on same-sex marriage, though activists denounced the abusive rhetoric employed by some campaigners (see Media, Diversity, and Content Manipulation)

## Introduction

The internet is categorized as “free” in Australia, though excessive penalties for online defamation and law enforcement agencies’ unfettered access to user metadata remain areas of concern.

Australians generally enjoy affordable, high-quality access to the internet and other digital media. Access has continued to expand over the past few years with the rollout of the National Broadband Network, though the government has been criticized for project’s slow and inconsistent implementation.

Content is freely available online, with no reports of blocking or filtering of political and social information. However, courts have awarded high damages for defamation, raising concerns that users may be pushed to self-censor as a result.

Social media became a battleground for fierce campaigning in the lead up to a polarizing national postal survey asking the Australian public whether same-sex

marriage should be legalized. Activists leveraged social media platforms to spread their message, though both sides complained they were subject to abuse online.

The government clarified in 2017 that metadata cannot be used as evidence in civil cases. However, concerns persist about law enforcement's otherwise unfettered access to user metadata, which telecommunication companies must store for two years. Though agencies must obtain a warrant to access metadata associated with accounts operated by journalists, incidents of unauthorized access have undermined faith in the protection.

## 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's 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, fiber to the node, and satellite services in rural communities. Although internet access is widely available in locations such as libraries, educational institutions, and cybercafes, Australians predominantly access the internet from home, work, and increasingly through mobile phones. <sup>1</sup>

Australians have a number of internet connection options, including ADSL, ADSL 2+, mobile, fixed wireless, cable, satellite, fiber, and dial-up. <sup>2</sup> As of June 2016, almost all of internet connections were broadband, while the number of dial-up connections declined to 90,000 out of a total of 13.3 million internet users. <sup>3</sup> By December, the number of internet users increased to 13.5 million. <sup>4</sup> Once fully implemented, the NBN is expected to make high-speed broadband available to Australians in remote and rural areas. <sup>5</sup>

However, the NBN project has increasingly grown to be a source of frustration for the Australian public. Initially framed as a project that would deliver universal fast internet across Australian communities, the slow and inconsistent rollout, complaints of slow speeds, and high public cost have increasingly fueled criticisms of the project. The federal government has implemented a program monitoring NBN speeds to verify that advertised speeds are accurate. <sup>6</sup> The NBN's completion date has been pushed back to 2020. <sup>7</sup>

Roughly 56.1 percent of all Australians have access to broadband speeds of 24 Mbps – 100 Mbps. <sup>8</sup> There are still parts of Australia experiencing slower broadband speeds (approximately 92,000 people have internet connection speeds below 1.5 Mbps). <sup>9</sup> Akamai ranked Australia 50th in the world for internet speed in 2016. <sup>10</sup>

As of December 31, 2016, the Australian Bureau of Statistics reported that there were 25.4 million mobile phone subscribers. <sup>11</sup> Fourth generation (4G) mobile services have driven recent growth, with all networks expanding coverage and the range of services on offer. <sup>12</sup>

Internet access is affordable for most Australians. However, the government has withdrawn a program subsidizing internet connections for individuals and small businesses in remote and rural areas, where internet access is less affordable due to higher prices and lower incomes. <sup>13</sup> Major internet service providers (ISPs) such as Telstra offer financial assistance to help low-income families connect to the internet. <sup>14</sup>

Rural and indigenous communities generally face more barriers to access. According to the 2011 Census, 63 percent of indigenous Australians report having an internet connection, compared with 77 percent of other households. <sup>15</sup>

November 27, 2012, <http://bit.ly/1F1ldX3>. The mobile phone penetration rate in indigenous communities is unknown.

One study attributed the lower rate of internet penetration in rural areas to the higher median age, larger populations of indigenous Australians, and higher unemployment rates in rural Australia. <sup>16</sup> (Older people are also less likely to use the internet: 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. <sup>17</sup>) However, the study did not assess internet use through mobile devices. <sup>18</sup> Telstra has committed to increasing coverage in rural areas, having invested in boosting its 4G service. <sup>19</sup>

Gender is not a barrier to accessing the internet, with approximately 85 percent of both males and females in urban areas accessing the internet in 2015. <sup>20</sup> In rural areas, 84 percent of females accessed the internet in the same period compared to 72 percent of males.

## Restrictions on Connectivity

The government does not impose restrictions on internet connectivity 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, also known as data shaping. Some Australian ISPs and mobile service providers practice traffic shaping under what are known as fair-use policies. If a customer is uses peer-to-peer file sharing software, internet connectivity for those activities will be slowed in order to release bandwidth for other applications. <sup>21</sup>

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 find themselves in a temporary “walled garden” or quarantine until they have communicated with the ISP and restored security. <sup>22</sup>

## ICT Market

Australia hosts a competitive market for internet access, with 63 providers as of December 2015, including ten very large ISPs (over 100,000 subscribers), 19 large ISPs (with 10,001 to 100,000 subscribers), and 34 medium ISPs (with 1,001 to 10,000 subscribers). <sup>23</sup>

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 carriage service providers do not require a license. **24** 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 (see Regulatory Bodies). **25**

Telstra is the dominant mobile provider, according to Roy Morgan Research. **26** As of October 2016, Telstra was leading the mobile market with a 39.1 percent market share, followed by Optus with 24.4 percent, and Vodafone with 19.4 percent.

## Regulatory Bodies

The Australian Communications and Media Authority (ACMA) is the primary regulator for the internet and mobile telephony. **27** Its oversight is generally viewed as fair and independent.

Australian ISPs are co-regulated under the Broadcasting Services Act (BSA) 1992, which combines regulation by the ACMA with self-regulation by the telecommunications industry. **28** The industry’s involvement consists of developing industry standards and codes of practice. **29** There are over 30 self-regulatory codes that govern and regulate Australian information and communication technologies (ICTs). ACMA approves self-regulatory codes negotiated among members of the Internet Industry Association (IIA). In March 2014, the Communications Alliance took over the responsibilities of the IIA through a signed agreement. **30**

Small businesses and residential customers may file complaints about internet, telephone, and mobile phone services with the Telecommunications Industry Ombudsman (TIO), **31** which operates as a free and independent dispute-resolution service.

Australia appointed its first cyber ambassador, Dr Tobias Feakin, in late 2016. Feakin’s role includes advocating for “an open and secure Internet.” He is tasked with

ensuring Australia has a strong and consistent stance on international cyber issues.

**32**

## B. Limits on Content

*There are relatively few limits to online content in Australia. Digital activism peaked in the lead up to the national survey on same-sex marriage, though some activists have complained of abusive rhetoric by campaigners.*

### Blocking and Filtering

Political and social content is not subject to blocking, and communications applications such as Facebook, Skype, and YouTube are freely available. Websites offering illegal services may be blocked or filtered under a narrow set of circumstances. However, the legal guidelines and technical practices by which ISPs filter illegal material have raised some concerns in the past.

Section 313(3) of the Telecommunications Act 1997 allows government agencies to block illegal online services. The application of the law proved controversial when the Australian Securities and Investment Commission (ASIC) used Section 313(3) to request ISPs to take down a fraudulent website. Several legitimate websites were blocked at the same time because their IP addresses were included in the request. **33** While the affected websites were swiftly restored, the matter led to a formal review of Section 313(3) in 2015. **34** The committee's final report was released on June 1, 2015 but has not prompted any change in the law or new guidelines to prevent collateral blocking. **35**

Copyright holders may apply to the Federal Court to request that overseas copyright infringing locations (websites and services) be blocked by Australian ISPs under the amended Section 115A of the Copyright Amendment (Online Infringement) Act 2015. **36** When making a decision, the court must take into consideration whether the overseas location has a primary purpose of facilitating copyright infringement, whether the response is proportionate, and whether or not blocking is in the public interest. **37** Popular websites that frequently host copyright infringing material,

including Pirate Bay and Kickass Torrents, were blocked in two recent Federal Court judgments. **38**

## Content Removal

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

Content restrictions by private companies periodically attract controversy. Facebook came under fire for censoring an ad run by an auction house, Mossgreen that featured the 1980 fine art painting, *Women Lovers*, by Australian artist Charles Blackman. **39** The painting features naked women and was considered to violate Facebook's restrictions on advertising adult products and services. Facebook declined Mossgreen's initial request to reconsider the decision, and only uncensored the ad after the issue attracted significant media coverage. **40**

A decision by the Supreme Court of South Australia in October 2015 had implications for intermediaries that enable internet users to access content created by others. The Court found that Google was liable for defamatory content about the plaintiff published by third party websites as a secondary publisher. The content was revealed in Google's search results, including through the search engine's autocomplete function, snippets of content displayed to help users choose between results, and hyperlinks to other websites. **41** Google was ordered to pay damages to the plaintiff.

**42** Reactions to the decision were mixed, but commentators raised concerns that it set a dangerous precedent, potentially encouraging claimants to censor legitimate criticism online, or making companies more likely to remove content to avoid defamation suits. **43** The Court dismissed Google's appeal in October 2017. **44**

## 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, including political campaigning and political protest. **45**

Additionally, the publicly-funded television station SBS features high quality news programs in multiple languages (available offline and online) to reflect the cultural diversity found in the Australian population.

In the lead up to a divisive 2017 postal survey conducted by the Australian Bureau of Statistics asking the Australian public whether same-sex marriage should be legalized, social media became host to fierce discussion and campaigning. The results of the survey will likely determine whether parliament legalizes same-sex marriage by the end of the year. Activists from both the “yes” and “no” camps have condemned the tone of the rhetoric online and reported that they had been subject to vilification by the other side. Those voting “no” against same-sex marriage said they were penalized for expressing their opinions on social media, including a children’s entertainer from Canberra who said she was fired from her job after posting on social media that “it’s OK to vote no.” **46** Meanwhile, “yes” voters have condemned the type of material circulated on social media by the “no” campaign, which frequently contained deliberately misleading, homophobic claims about the LGBTI community. Some online advertising paid for by “no” campaigners claimed that gay parenting harms children, linked same-sex marriage to a globalist conspiracy by billionaire philanthropist George Soros, and claimed that same-sex marriage would lead to the indoctrination of school children. **47**

In response to complaints that campaigning was turning vicious, the Australian parliament enacted the Marriage Law Survey (Additional Safeguards) Act in September 2017 making it an offence to vilify, intimidate, or threaten a person because of their views in relation to the same-sex marriage survey or because of their religion, sexual orientation, gender identity, or intersex status. The law has a sunset clause and will be in effect only until November 15 2017, after the survey is complete. **48**

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 regulating hate speech or racial vilification (see Legal Environment). **49** Nevertheless, fear of being accused of defamation (and, to a

lesser extent, contempt of court) has driven some self-censorship by both the media and ordinary users. For example, narrowly written orders to suppress coverage of ongoing legal proceedings are often interpreted by the media in an overly broad fashion so as to avoid contempt of court charges. **50**

## Digital Activism

Australians use social media to sign petitions to the government, and to mobilize for public protest. Following a “Women’s March On Washington” event to promote human rights and end bigotry, a Sydney march with similar aims of supporting women and minorities was organized through social media. **51** Earlier popular protests included rallying against the closure of aboriginal communities in Western Australia **52** and protests at the G20 Summit in Brisbane. **53**

In a precedent setting case, Sydney man Zane Alchin was handed down a one-year good behavior bond in July 2016 after being charged with using a carriage service to menace. Alchin had written abusive, sexually charged comments on Facebook towards several women. **54** The women at the center of the case launched an online advocacy group “Sexual Violence Won’t be Silenced” to rally support for the case against Alchin, as well as lobbying for law reform and for the allocation of proper training and resources in the fight against sexual abuse against women online. **55**

In the lead up to Australia Day in January 2017, some Australian social media users mobilized around the #ChangeTheDate hashtag. Change the Date is an ongoing campaign to change Australia’s national day as part of an effort to recognize injustices done to the indigenous population. **56**

## 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

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. 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. **57**

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 that is 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. **58** Observers have noted that defamation suits for content posted online have become more common than claims against traditional media, meaning ordinary social media users can find themselves within reach of the courts. **59** Civil actions over defamation 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. **60**

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. While the United States and the United Kingdom have enacted laws to restrict libel tourism, Australia is

not currently considering any such legislation. In some cases, the courts may grant a permanent injunction to prevent the publication of defamatory material, though this remedy is limited to cases where there is a high risk of the continuation of the defamation. <sup>61</sup>

## Prosecutions and Detentions for Online Activities

A number of lawsuits involving defamation online have made the headlines in recent years. While the cases were not characterized as attempts to suppress information that was accurate and in the public interest, some observers said the heavy financial penalties involved could deter investigative reporting and free speech (see Media, Diversity, and Content Manipulation).

In October 2016, a West Australian judge ordered former police officer Terence McLernon to pay AUD \$700,000 (US\$500,000) in damages for defaming three businessmen, including Anton Billis, managing director of mining companies Rand Mining and Tribune Resources. The judge found that McLernon's blog posts, which accused the men of being part of an organized crime gang and of firebombing McLernon's house and car, had exposed the plaintiffs and their companies to financial risk caused by negative publicity. <sup>62</sup>

In a November 2015 trial, a jury found that a barrister had defamed a police officer through comments he posted on a website in 2012. The officer, Sergeant Colin Dods, was involved in the death of an armed teenager. The coroner found that Dods did not cause the death directly, and that several officers had fired on the young man because they were at risk of serious injury. Queensland barrister Michael McDonald accused Dods of manslaughter in a series of online comments. <sup>63</sup> The jury found the comments were defamatory, leading Justice Bell to award Dods aggravated damages totalling AUD \$150,000 (USD \$114,000) based on the level of harm caused. <sup>64</sup>

In a separate case from January 2015, a Western Australian court ordered Robyn Greeuw to pay AUD \$12,500 (US\$8,900) in damages for Facebook posts alleging that her former husband Miro Dabrowski had abused her. <sup>65</sup> The defense of truth was not proven.

The 2013 case of *Mickle v Farley*,<sup>66</sup> where a young man in New South Wales was fined AUD \$105,000 (US\$93,400) plus costs for posting defamatory statements on Twitter and Facebook about his music teacher, was widely publicized. The case was novel for the amount of damages awarded, and for being the first Australian decision where a tweet was held to be defamatory.<sup>67</sup> 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.”<sup>68</sup>

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 without consent, known as “revenge porn” because it is typically carried out by former partners. In 2012, for example, Ravshan Usmanov pled guilty to publishing an indecent article and was sentenced to six months of home detention after he posted nude photographs of an ex-girlfriend on Facebook.<sup>69</sup> An appeal court commuted the original sentence and suspended the detention. In 2017, the state of New South Wales introduced an amendment to the Crimes Act criminalizing the recording and distribution of revenge porn, with penalties of up to AUD \$11,000 and three years in prison.<sup>70</sup>

## 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).

<sup>71</sup> 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. **72** Unlawful collection and disclosure of the content of a communication can draw both civil and criminal sanctions. **73** The TIAA and TA explicitly authorize a range of disclosures, including to specified law enforcement and tax agencies. ISPs are currently able to monitor their networks without a warrant for “network protection duties,” such as curtailing malicious software and spam. **74**

In a troubling development, law enforcement agencies no longer require a warrant to access 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 to 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. Telecommunications companies were required to update their technology so as to be compliant with the law by April 2017, receiving a substantial grant from the government to assist with the process. **75** In a recent development to the Act, during April 2017, the government announced metadata will be excluded from being used in civil cases.

Amendments to the law in 2015 added extra privacy protections to journalists, requiring security agencies to obtain a warrant before accessing journalists' metadata. However, incidents of unauthorized access have undermined faith in the protection afforded to journalists. In April 2017, the Australian Federal Police (AFP) reported to the Commonwealth Ombudsman, which oversees complaints involving government agencies, that they had accidentally accessed a journalist's metadata without a warrant. Journalists have expressed frustration that the officers involved were not subject to disciplinary processes. **76**

In February 2016, investigative journalist Paul Farrell of *The Guardian Australia* discovered that the AFP had retrieved metadata associated with his devices without a warrant in an apparent attempt to identify the source behind a 2014 story on a controversial government policy regarding asylum seekers. **77** 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.” **78**

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. **79** The controversial amendment prompted the independent national security legislation monitor, Robert Gyles QC, to specifically assess the impact of section 35P on journalists in October 2015. Gyles' report concluded that section 35P 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. **80** The government announced their intention to support the six recommendations included in Gyle's report to better protect journalists and their sources, **81** but had yet to amend the law. 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.

Law enforcement agencies also make requests to international companies. Google's transparency report for the second half of 2016 reveals that Australian law enforcement made 1,407 user data requests from the company. Google handed over some data in 67 percent of cases.

In the midst of renewed debate over encryption, Prime Minister Malcom Turnbull announced that new laws may be introduced in the near future that would force companies to allow law enforcement to access encrypted communications. **82** The announcement was met with criticism, with concerns that such laws would entail backdoor access and weakened security on popular platforms. **83** Meanwhile, April

2015 revisions to the Defense Trade Controls Act 2012 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. **84**

Nonetheless, 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 with a valid warrant. **85**

## Intimidation and Violence

Violence against online commentators is rare in Australia. Controversial figures are occasionally subject to intimidation and death threats online. Joshua Goyne, a gay rodeo bull rider from rural Australia, reported receiving abusive messages and death threats on online forums in 2017. **86**

## Technical Attacks

Cyberattacks and hacking incidents remain a common concern in Australia, though they generally target larger institutions and have not been widely used to censor online speech or punish government critics.

Some cause significant disruptions, however. In April 2017, Australian domain name registration company Melbourne IT suffered a major DDoS attack rendering approximately 500,000 websites inaccessible access for around 90 minutes. The company stated that the attack originated from overseas. **87**

The global “Petya” ransomware attack affected some Australian business in June 2017, including the offices of large law firm DLA Piper. Infected computers were locked, and demanded a payment in order to restore access. The effect of the virus was relatively limited in Australia and quickly contained. **88** Another high-profile

global ransomware phenomenon, WannaCry, had relatively little impact in Australia, though a small number of businesses were affected. <sup>89</sup> Telecommunications giant Telstra reported that 60 percent of Australian businesses had experienced at least one ransomware incident within a one year period. <sup>90</sup>

A “state-sponsored cyber adversary” reportedly infected the Australian Bureau of Meteorology network with malware in 2015. Experts speculated that the attack had strategic and commercial motivations. <sup>91</sup> Banks have also fallen victim to cyberattacks, and hackers attempted to steal two-factor authentication codes protecting the accounts of customers with four major banks in 2016. <sup>92</sup>

According to the Australian Cyber Security Centre, the Computer Emergency Response Team responded to 14,804 cyberattack incidents between 2015 and 2016. <sup>93</sup> Targets included businesses, non-governmental agencies, and the Australian government.

## Footnotes

- 1 Australian Bureau of Statistics (ABS), “8146.0 - Household Use of Information Technology, Australia, 2014-2015: Personal internet use,” February 18, 2016, <http://bit.ly/1Nyo7ND>.
- 2 ABS, “8153.0 – Internet Activity, Australia, December 2016: Type of Access Connection,” April 5, 2017, <http://bit.ly/1Mq3ouD>.
- 3 Ibid.
- 4 Ibid.
- 5 NBN Co, “NBN set to narrow digital divide for 400,000 homes and businesses,” media release, February 9, 2015, <http://bit.ly/16VvWwl>.

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

### In Other Reports

Freedom in the World 2017

### Other Years

2020

**Be the first to  
know what's  
happening.**

Email

Join the Freedom House  
monthly newsletter

Subscribe

#### ADDRESS

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

#### GENERAL INQUIRIES

[info@freedomhouse.org](mailto:info@freedomhouse.org)

#### PRESS & MEDIA

[press@freedomhouse.org](mailto:press@freedomhouse.org)

@2020 FreedomHouse