

# Australia

Free

77

100

A [Obstacles to Access](#) 23 25

B [Limits on Content](#) 29 35

C [Violations of User Rights](#) 25 40

Last Year's Score & Status

79 100 Free



## Overview

Internet freedom in Australia declined during the coverage period. The country's information and communication technology (ICT) infrastructure is well developed, and prices for connections are low, ensuring that much of the population enjoys access to the internet. However, a number of website restrictions, such as those related to online piracy or "abhorrent" content, limit the content available to users. The March 2019 terrorist attack on mosques in Christchurch, New Zealand, prompted internet service providers (ISPs) to block certain websites and the

government subsequently introduced a new law that criminalized the failure to delete “abhorrent” content. Other legal changes—including court decisions expanding the country’s punitive defamation standards, an injunction silencing digital media coverage of a high-profile trial, and a problematic law that undermines encryption—shrank the space for free online expression in Australia. Finally, an escalating series of cyberattacks sponsored by China profoundly challenged the security of Australia’s digital sphere.

Australia is a democracy with a strong record of advancing and protecting political rights and civil liberties. Recent challenges to these freedoms have included the threat of foreign political influence, harsh policies toward asylum seekers, and ongoing disparities faced by indigenous Australians.

## Key Developments

### June 1, 2018 - May 31, 2019

- After the March 2019 Christchurch attack, in which an Australian man who had espoused white supremacist views allegedly killed 51 people at two New Zealand mosques, ISPs acted independently to block access to more than 40 websites that hosted the attacker’s live-streamed video of his crimes. The blocks remained in place for the duration of the coverage period ([see B1](#)).
- In April 2019, Parliament passed the Sharing of Abhorrent Violent Material Act, which established criminal penalties for failure to remove a new category of illicit online content ([see B2](#) and [B3](#)).
- A court injunction prohibited reporting on the trial of Cardinal George Pell, who was convicted on charges of sexual abuse in December 2018; any online journalists who violated the order would face contempt of court charges ([see B4](#)).
-

In December 2018, Parliament passed the Telecommunications and Other Legislation Amendment (Assistance and Access) Act, which empowered authorities to access encrypted user data, among other provisions ([see C4](#)).

- The government reported in February 2019 that a “sophisticated state actor” had hacked the computer networks of Parliament and the country’s major political parties ([see C8](#)).

## A Obstacles to Access

*There are few obstacles to internet access in Australia. Service continues to improve in remote and rural areas throughout the country, and the gradual rollout of the National Broadband Network is driving prices down to some extent. The ICT sector is mature and competitive, generally providing Australians with high-quality internet connectivity.*

A1 0-6 pts

Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?

66

There are few infrastructural limitations on internet access or speeds. The country has a high internet penetration rate: some 86.6 percent of the population used the internet in 2018, per International Telecommunication Union (ITU) data.<sup>1</sup> This rate is expected to steadily increase with the implementation of the National Broadband Network (NBN) program, which entails expanded wireless, fiber-optic, and satellite internet services, especially in rural communities. The NBN is starting to deliver faster connections to more residents at lower costs, but it has been dogged by complaints and delays.<sup>2</sup> In May 2019 the Australian Competition and Consumer Commission (ACCC) reported that while NBN speeds had improved in the previous quarter, some NBN users experienced frequent outages and slower-than-advertised download speeds.<sup>3</sup> The NBN’s completion date, initially scheduled for 2016–17, has been pushed back to 2020.<sup>4</sup>

Users generally access the internet through desktop or laptop computers and smartphones.<sup>5</sup> There are a number of internet connection options, including cable,

dial-up, DSL (digital subscriber line), fiber-optic, mobile, and satellite services.<sup>6</sup> As of December 2018, almost all internet connections in the country were broadband. The ACC recorded about 7.2 million fixed-line broadband subscriptions and 8.4 million wireless broadband subscriptions.<sup>7</sup> By January 2019, the number of internet users had reached 21.74 million, in a country of about 25 million people.<sup>8</sup>

Most users rely on download speeds of 24 Mbps or less, while just 5 percent access the internet via connections with download speeds of 100 Mbps or more.<sup>9</sup> Ookla's May 2019 Speedtest Global Index ranked Australia 59th in the world for fixed-line broadband internet speeds, but fifth in the world for mobile broadband internet speeds.<sup>10</sup>

Third- and fourth-generation (3G and 4G) mobile networks cover 99.4 percent of the population in terms of geographical reach.<sup>11</sup> Providers Telstra and Optus have started offering limited 5G services in some areas, with coverage due to expand through 2020. Vodafone has indicated that it will start offering 5G in 2020.<sup>12</sup> In August 2018, Huawei, the Chinese telecommunications giant, was barred from participating in the development of Australia's 5G network. Critics are concerned that the ban, which was imposed on national security grounds, will result in slower 5G internet speeds and delays in the rollout of the service.<sup>13</sup>

- [1. https://www.itu.int/net4/itu-d/icteye/CountryProfileReport.aspx?country...](https://www.itu.int/net4/itu-d/icteye/CountryProfileReport.aspx?country...)
- [2. Australian Competition and Consumer Commission, 'Communications Market Report 2017-18' https://www.accc.gov.au/publications/accc-telecommunications-report/acc...](https://www.accc.gov.au/publications/accc-telecommunications-report/acc...)
- [3. Australian Competition and Consumer Commission, 'NBN Speeds Improving, But More Work to Do,' May 7, 2019 https://www.accc.gov.au/media-release/nbn-speeds-improving-but-more-wor...](https://www.accc.gov.au/media-release/nbn-speeds-improving-but-more-wor...)
- [4. "Federal election: NBN promises past and present, explained," ABC News June 13, 2016, https://www.abc.net.au/news/2016-06-13/federal-election-nbn-promises-pa...](https://www.abc.net.au/news/2016-06-13/federal-election-nbn-promises-pa...)
- [5. ABS, "Household Use of Information Technology, Australia, 2016-17: Devices Used to Access the Internet at Home," March 28, 2018, http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/8146.0Main+Features12016...](http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/8146.0Main+Features12016...)
- [6. ABS, "Internet Activity, Australia, December 2017: Type of Access Connection," April 3, 2018, https://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/8153.0Main+Features1Dec...](https://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/8153.0Main+Features1Dec...)
- [7.](#)

- [https://www.accc.gov.au/system/files/1567\\_Internet%20activity%20report%...](https://www.accc.gov.au/system/files/1567_Internet%20activity%20report%...)
- [8. https://www.roi.com.au/blog/australian-internet-social-media-statistics...](https://www.roi.com.au/blog/australian-internet-social-media-statistics...)
- [9.](#)
- [https://www.accc.gov.au/system/files/1567\\_Internet%20activity%20report%...](https://www.accc.gov.au/system/files/1567_Internet%20activity%20report%...)
- [10. http://web.archive.org/web/20190629201034/https://speedtest.net/global-...](http://web.archive.org/web/20190629201034/https://speedtest.net/global-...)
- [11. Australian Communications and Media Authority \(ACMA\), 'Communications Report 2017-18,' https://www.acma.gov.au/-/media/Research-and-Analysis/Report/pdf/Commun...](https://www.acma.gov.au/-/media/Research-and-Analysis/Report/pdf/Commun...)
- [12. "What is 5G and when is it coming to Australia," Choice, 24 January 2019 https://www.choice.com.au/electronics-and-technology/internet/connectin...;](https://www.choice.com.au/electronics-and-technology/internet/connectin...)  
"When is 5G coming to Australia," Lifewire, 1 July 2019  
<https://www.lifewire.com/5g-australia-4583137>
- [13. https://theconversation.com/blocking-huawei-from-australia-means-slower...](https://theconversation.com/blocking-huawei-from-australia-means-slower...)

A2 0-3 pts

Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons? 23

Internet access is affordable for most Australians. The gradual shift to NBN services across the country is resulting in greater competition among ISPs, higher-quality connections, and improved speeds.<sup>1</sup> The number of premises with active NBN connections increased to 4 million in 2017–18.<sup>2</sup>

Telecommunications services are becoming cheaper, with the ACCC reporting a 1.5 percent decrease in the annual price of a fixed-line broadband connection and a 7.5 percent decrease in the annual price of a mobile broadband connection in 2017–18.<sup>3</sup> In the 2019 Inclusive Internet Index, Australia was ranked fourth out of 100 countries surveyed in terms of the affordability of prices for internet connections.<sup>4</sup>

A digital divide persists between urban and nonurban areas, though it is narrowing. According to 2018 Australian Bureau of Statistics data, 77 percent of households in “remote or very remote” areas have access to the internet, compared with 88 percent of households in major cities.<sup>5</sup> The NBN is intended to make high-speed broadband service available to residents of nonurban areas,<sup>6</sup> and as of 2018, these areas accounted for 55 percent of active NBN connections.<sup>7</sup>

One study attributed the lower rate of internet penetration in rural areas to the higher median age, larger populations of disadvantaged indigenous Australians, and

higher unemployment rates.<sup>8</sup> In general, indigenous people and people with disabilities tend to have lower levels of internet access and digital literacy.<sup>9</sup> The number of older people using the internet has grown over the past few years, though the over-65 age group remains significantly less likely to use the internet. Ninety-eight percent of Australians between the ages of 15 and 17 are internet users, compared with only 55 percent of those older than 65.<sup>10</sup>

Nonurban areas also feature less thorough mobile coverage than urban areas. The federal government as well as some state governments are working in conjunction with mobile service providers to improve coverage in regional blackspots.<sup>11</sup>

Gender is not a barrier to access, with men using the internet only slightly more frequently than women.<sup>12</sup>

- <sup>1</sup>. Australian Communications and Media Authority (ACMA), 'Communications Report 2017-18,' <https://www.acma.gov.au/-/media/Research-and-Analysis/Report/pdf/Commun...>
- <sup>2</sup>. Australian Communications and Media Authority (ACMA), 'Communications Report 2017-18,' <https://www.acma.gov.au/-/media/Research-and-Analysis/Report/pdf/Commun...>
- <sup>3</sup>. Australian Competition and Consumer Commission, 'Communications Market Report 2017-18,' <https://www.accc.gov.au/system/files/ACCC%20Communications%20Market%20R...>
- <sup>4</sup>. <https://theinclusiveinternet.eiu.com/explore/countries/AU/performance/i...>
- <sup>5</sup>. ABS, "Household Use of Information Technology, Australia, 2016-17: Household Internet Access," March 28, 2018, <http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/8146.0Main+Features12016...>
- <sup>6</sup>. NBN Co, "NBN set to narrow digital divide for 400,000 homes and businesses," February 9, 2015, <http://bit.ly/16VvWwl>
- <sup>7</sup>. Australian Communications and Media Authority (ACMA), 'Communications Report 2017-18,' <https://www.acma.gov.au/-/media/Research-and-Analysis/Report/pdf/Commun...>
- <sup>8</sup>. Sora Park, "Digital inequalities in rural Australia: A double jeopardy of remoteness and social exclusion," Journal of Rural Studies, January 13, 2015, 5, <http://bit.ly/2pEiqIV>
- <sup>9</sup>. State of Digital Rights <https://digitalrightswatch.org.au/wp-content/uploads/2018/05/State-of-D...>
- <sup>10</sup>. ABS, "Household Use of Information Technology, Australia, 2016-17:

Internet Access by Persons,” March 28, 2018,

<http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/8146.0Main+Features12016...>

- [11.](#) Australian Communications and Media Authority (ACMA), ‘Communications Report 2017-18,’ <https://www.acma.gov.au/-/media/Research-and-Analysis/Report/pdf/Commun...>
- [12. https://theinclusiveinternet.eiu.com/explore/countries/performance/avai...](https://theinclusiveinternet.eiu.com/explore/countries/performance/avai...)

A3 0-6 pts

Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?

66

The government does not impose restrictions on internet connectivity or mobile networks.

Australia is connected to the international internet through undersea cables that are not controlled by the government.[1](#) Domestically, internet traffic flows through either commercial or nonprofit internet exchange points (IXPs),[2](#) which are located in most major cities.[3](#)

Under the iCode, a set of voluntary cybersecurity guidelines for ISPs, internet connectivity may be temporarily restricted for users whose devices have become part of a botnet—an array of computers that have been hijacked for use in coordinated cyberattacks or spam distribution—or are at high risk of being infected with malicious software. Such users may have their internet service temporarily throttled or find themselves in a “walled garden,” or quarantine, until they have communicated with their ISP and restored security.[4](#)

The 1997 Telecommunications Act places obligations on providers to assist authorities in certain circumstances, including restricting the provision of services in emergencies.[5](#)

- [1. https://www.submarinecablemap.com/#/country/australia](https://www.submarinecablemap.com/#/country/australia)
- [2. https://www.pch.net/ixp/dir#!mt-filters=%7B%22ctry%22%3A%5B%22dropdown%...](https://www.pch.net/ixp/dir#!mt-filters=%7B%22ctry%22%3A%5B%22dropdown%...)
- [3. https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018...](https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018...)
- [4.](http://bit.ly/1GhwClm) Communications Alliance Ltd, “Industry Code C650:2014 iCode: Internet Service Providers Voluntary Code of Practice for Industry Self-Regulation in the Area of Cybersecurity,” 2014, <http://bit.ly/1GhwClm>
- [5.](https://www.legislation.gov.au/Details/C2019C00104) Telecommunications Act 1997, <https://www.legislation.gov.au/Details/C2019C00104>

, See sections 313-315 and Divisions 3 and 4

A4 0-6 pts

Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?

56

The ISP sector is free of major legal, regulatory, and economic obstacles that might restrict the diversity of service providers. However, telecommunications giant Telstra has consistently held the largest share of the mobile and broadband markets.

Australia hosts a competitive market for internet access, with 63 providers as of mid-2017, including nine very large ISPs (with more than 100,000 subscribers), 22 large ISPs (with 10,001 to 100,000 subscribers), and 32 medium ISPs (with 1,001 to 10,000 subscribers).<sup>1</sup> Telstra commands over 60 percent of the fixed-line broadband market, with TPG, Optus, and Vocus holding smaller shares.<sup>2</sup> All four leading ISPs sell NBN connections. As of 2018, Telstra controlled a 53.6 percent share of the mobile service market, followed by Optus with 29.2 percent and Vodafone with 17.2 percent.<sup>3</sup>

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.<sup>4</sup> Larger ISPs that own telecommunications infrastructure, or “carriers,” are required to obtain operating licenses from the Australian Communications and Media Authority (ACMA) ([see A5](#)). They must also submit to dispute resolution by the independent Telecommunications Industry Ombudsman (TIO).<sup>5</sup>

- [1.](https://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/8153.0Main+Features1Jun...)
- [2.](https://www.acma.gov.au/-/media/Research-and-Analysis/Report/pdf/Commun...) Australian Communications and Media Authority (ACMA), 'Communications Report 2017-18,'
- [3.](https://www.acma.gov.au/-/media/Research-and-Analysis/Report/pdf/Commun...) Australian Communications and Media Authority (ACMA), 'Communications Report 2017-18,'
- [4.](https://www.acma.gov.au/-/media/Networks/Publication/pdf/Know-Your-Tele...)
- [5.](https://www.acma.gov.au/-/media/Networks/Publication/pdf/Know-Your-Tele...)

A5 0-4 pts

Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?

44

ACMA is the primary regulator for the broadcasting, internet, and telecommunications sectors.<sup>1</sup> Its oversight is generally viewed as fair and independent. ACMA members are formally appointed by the governor general of Australia (who in turn is appointed by the monarch on the recommendation of the prime minister and is advised by the government) for five-year terms.<sup>2</sup>

Australian ISPs are coregulated under the Broadcasting Services Act (BSA) of 1992, which combines regulation by the ACMA with self-regulation by the telecommunications industry.<sup>3</sup> The industry's involvement entails developing industry standards and codes of practice.<sup>4</sup> There are more than 30 self-regulatory codes that govern and regulate the country's ICTs. ACMA approves self-regulatory codes produced by the Communications Alliance, Australia's main telecommunications industry body.<sup>5</sup>

Small businesses and residential customers may file complaints about internet, telephone, and mobile phone services with the TIO,<sup>6</sup> which operates a free and independent dispute-resolution mechanism.

The government appointed its first “ambassador for cyber affairs,” Tobias Feakin, in late 2016. Feakin’s role includes advocating for “an open and secure internet.” He is tasked with ensuring that Australia has a strong and consistent stance on international cyber issues.<sup>7</sup>

- [1. https://www.acma.gov.au/theACMA/About/Corporate/Structure-and-contacts/...](https://www.acma.gov.au/theACMA/About/Corporate/Structure-and-contacts/...); <https://www.acma.gov.au/theACMA/About/Corporate/Responsibilities/regula...>
- [2. https://www.legislation.gov.au/Details/C2018C00353](https://www.legislation.gov.au/Details/C2018C00353)
- [3.](#) Australian Communications and Media Authority Act 2005, <http://bit.ly/1jz1CyZ>; Broadcasting Services Act 1992, <http://bit.ly/1VneSrn>; <https://www.acma.gov.au/Industry/Telco/Carriers-and-service-providers/L...>
- [4.](#) 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>
- [5.](#) Communications Alliance, “Internet Service Provider Industry,” <http://bit.ly/1LPtIRq>
- [6.](#) Telecommunications Industry Ombudsman, <http://www.tio.com.au>
- [7. https://www.zdnet.com/article/dr-tobias-feakin-appointed-as-australias-...](https://www.zdnet.com/article/dr-tobias-feakin-appointed-as-australias-...)

## B Limits on Content

*There are few restrictions on online content in Australia, but ISPs and the government took steps to curb certain types of violent material in the wake of the March 2019 terrorist attack in New Zealand, and a new law on the topic raised concerns that ISPs could be motivated to err on the side of censorship in order to avoid penalties.*

B1 0-6 pts

Does the state block or filter, or compel service providers to block or filter, internet content?

56

Political and social content is rarely subject to blocking, and communications applications and social media are freely available. However, popular websites that frequently host copyright-infringing material, including Pirate Bay and Kickass Torrents, were blocked by two Federal Court judgments from 2016 and 2017.<sup>1</sup>

During the 2018–19 coverage period, owners of copyrighted material continued to enjoy success in enforcing website blocking injunctions. The websites subjected to recent injunctions, such as Demonoid, LimeTorrents, EZTV, and Project FreeTV, facilitated downloading or streaming of copyright-infringing material.<sup>2</sup>

Although the Australian government did not order any website blocks in the wake of the March 2019 terrorist attack in Christchurch, New Zealand, several major Australian ISPs temporarily restricted access to 4chan, 8chan, LiveLeak, Voat, ZeroHedge, and other, smaller websites that were believed to be hosting or sharing recordings of the attacker’s live-streamed video.<sup>3</sup> Major social media platforms on which the live stream was also being disseminated were not blocked. The ISPs initially acted independently, but they later coordinated with ACMA and other government agencies.<sup>4</sup> Critics raised concerns regarding the lack of transparency and oversight of the blockings.<sup>5</sup> The restrictions reportedly remained in effect for the remainder of the coverage period; only in September 2019 did the Office of the eSafety Commissioner “clear the way” for ISPs to undo the blocks on all but eight unspecified websites that “continue to provide access to the video of the Christchurch terrorist attacks or the manifesto of the alleged perpetrator.”<sup>6</sup> There was no official, publicly available list of blocked websites. According to news reports, 43 sites were originally blocked.<sup>7</sup>

- <sup>1</sup>. Roadshow Films Pty Ltd v Telstra Corporation Ltd [2016] FCA 1503 (15 December 2016); Universal Music Australia Pty Limited v TPG Internet Pty Ltd [2017] FCA 435 (28 April 2017).
- <sup>2</sup>. [http://www.copyright.org.au/acc\\_prod/ACC/Information\\_Sheets/Copyright I...](http://www.copyright.org.au/acc_prod/ACC/Information_Sheets/Copyright_I...)
- <sup>3</sup>. <https://arstechnica.com/tech-policy/2019/03/australian-and-nz-isps-bloc...>
- <sup>4</sup>. <https://www.sbs.com.au/news/telcos-block-access-to-websites-continuing-...>; <https://www.smh.com.au/business/companies/telco-giants-block-websites-s...>
- <sup>5</sup>. <https://www.innovationaus.com/2019/03/Arbitrary-site-blocks-a-worrying-...>
- <sup>6</sup>. <https://www.esafety.gov.au/about-the-office/newsroom/media-releases/pro...>
- <sup>7</sup>. <https://www.theguardian.com/technology/2019/sep/09/australian-internet-...>

B2 0-4 pts

Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content?

24

Online content protected under international human rights standards is generally

free from interference by state and nonstate actors. However, the courts sometimes attempt to inhibit publication of defamatory material on large social media platforms and search engines.

In April 2019, Parliament adopted the Sharing of Abhorrent Violent Material Act ([see B3](#)), which amends the criminal code to enforce the removal of a new category of online content, namely “abhorrent violent material.” According to a September 2019 New York Times article, the Office of the eSafety Commissioner had received “30 or so” reports in relation to the new law, and “only five have led to notices against site owners and hosts.”[1](#) In response, two site owners and hosts removed reported content.

In its most recent transparency report, covering July to December 2018, Facebook disclosed that it had restricted access to 204 items of content (203 posts and one comment) in Australia.[2](#) Of these, 184 were alleged by the electoral commission in the state of Victoria to have violated local election laws, and one item was flagged by the Office of the eSafety Commissioner for cyberbullying. Eighteen takedowns related to “private reports of defamation.” Meanwhile, the government sent Google 24 content-removal requests, citing reasons including bullying and harassment (5 requests), defamation (8 requests), nudity and/or obscenity (3 requests), national security (1 request), and “privacy and security” (7 requests), during the same period.[3](#) These requests covered 181 items, mainly search results. Google complied with these requests 46 percent of the time. The government sent Twitter 14 takedown requests in the latter half of 2018, targeting 20 individual accounts.[4](#) Twitter complied with these requests 15 percent of the time.

Recent court cases involving Google’s search results and autocomplete predictions have sought to clarify how Australia’s defamation laws are applied to online content.

In June 2018, the High Court of Australia upheld an appeal brought by Milorad Trkulja against Google after a lower court dismissed the appellant’s defamation case in 2017.[5](#) The appellant argued that the Google autocomplete predictions and image searches related to his name were defamatory, as they linked him to infamous organized crime figures. The High Court agreed that the search results had the ability to convey to an ordinary, reasonable person that the appellant was linked to the criminal underworld.[6](#) The case was expected to return to the Supreme Court of Victoria for trial.[7](#)

In an older case involving a breach of confidential information, Twitter was ordered to prevent an offending user from creating any future accounts or posts, with worldwide effect. In 2017, the Supreme Court of New South Wales issued the global injunction against Twitter in relation to a series of tweets published by an anonymous user that revealed confidential information about the plaintiff, an unidentified company. Justice Michael Pembroke, having found that the court possessed the necessary jurisdiction to grant an injunction against Twitter, ordered that the service be restrained from allowing any future publication of the offending material and required to remove any instances of the offending material and any accounts associated with the user in question. Twitter had argued that it would not be feasible to proactively monitor user content, but the court held that Twitter had failed to provide an adequate explanation of this claim and proceeded instead on the assumption that Twitter possessed a content-filtering mechanism.<sup>8</sup> Commentators reacted to the decision with some concern, noting that its severity could validate the online censorship practices of undemocratic regional neighbors like China.<sup>9</sup>

In 2015, the Supreme Court of South Australia found Google liable as a secondary publisher of defamatory content that was initially published by third-party websites. The content was revealed in Google's search results, including through the search engine's autocomplete function, in snippets of content displayed to help users choose between results, and via hyperlinks to other websites.<sup>10</sup> Google was ordered to pay damages to the plaintiff.<sup>11</sup> 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.<sup>12</sup> The court dismissed Google's appeal in 2017.<sup>13</sup>

- [1. https://www.nytimes.com/2019/09/11/world/australia/internet-extremist-v...](https://www.nytimes.com/2019/09/11/world/australia/internet-extremist-v...)
- [2. https://transparency.facebook.com/content-restrictions/country/AU](https://transparency.facebook.com/content-restrictions/country/AU)
- [3. https://transparencyreport.google.com/government-removals/by-country/AU](https://transparencyreport.google.com/government-removals/by-country/AU)
- [4. https://transparency.twitter.com/en/countries/au.html](https://transparency.twitter.com/en/countries/au.html)
- [5. https://globalfreedomofexpression.columbia.edu/cases/trkulja-v-google-l...](https://globalfreedomofexpression.columbia.edu/cases/trkulja-v-google-l...)
- [6. Milorad Trkulja \(Aka Michael Trkulja\) V Google Llc \[2018\] HCA 25, Judgment Summary, http://www.hcourt.gov.au/assets/publications/judgment-summaries/2018/hc...](http://www.hcourt.gov.au/assets/publications/judgment-summaries/2018/hc...)
- [7. ABC News, 'High Court allows Milorad Trkulja to sue Google for defamation](#)

over images linked to crime bosses' 13 June 2018,

<http://www.abc.net.au/news/2018-06-13/milorad-trkulja-sues-google-for-d...>

- [8.](#) X v Twitter Inc [2017] NSWSC 1300  
<https://www.caselaw.nsw.gov.au/decision/59cad2be4b074a7c6e18fa3>
- [9.](#) 'The exorbitant injunction in X v Twitter', Michael Douglas, January 2017, Communications Law Bulletin.
- [10.](#) Duffy v Google Inc [2015] SASC 170.
- [11.](#) Candice Marcus, "Google ordered to pay Dr Janice Duffy \$100,000 plus interest in defamation case," Abc news, December 23, 2015,  
<http://ab.co/2exdcaL>
- [12.](#) Landers & Rogers Lawyers, "Duffy v Google - is this the end of the internet as we know it?" Defamation Bulletin, October 30, 2015, <http://bit.ly/2pH4oby>; "Australian court rules that Google is liable for defamatory links," TechnoLlama, October 30, 2015, <http://bit.ly/2qraBZY>
- [13.](#) "Supreme Court: Google left open to defamation suits after dismissal of appeal against Dr Janice Duffy," The Advertiser, October 4, 2017,  
<http://bit.ly/2ABBgpt>

B3 0-4 pts

Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?

24

Australia is home to a limited but increasing number of restrictions on the internet. Websites that offer illegal services such as interactive gambling may be blocked or filtered under a narrow but expanding set of circumstances.<sup>1</sup> The legal and technical mechanisms by which ISPs filter illegal material have raised some concerns. During the coverage period, the amendments to the criminal code in response to the Christchurch attack introduced an expansive new category of online content that social media companies must remove, while an amendment to the 1968 Copyright Act opened up more avenues for blocking or removing copyright-infringing material.

Concerns persist over ISPs' blocking of websites that hosted footage of the Christchurch attack. Critics contended that these blocks were not transparent, proportional, or—because they were imposed by private companies instead of the government—appropriate.<sup>2</sup> In a public statement, Telstra acknowledged that the blocks "may inconvenience some legitimate users of these sites." Vodafone issued

a similar acknowledgment.[3](#)

While ISPs implemented those blocks on their own initiative, the government secured Parliament's approval in April 2019 for amendments to the criminal code that required ISPs, along with "content service providers," and "hosting service providers," to "expeditiously" remove any "abhorrent violent material," defined as content depicting attempted murder, murder, terrorism, torture, rape, or kidnapping, that is accessible in Australia.[4](#) The Office of the eSafety Commissioner may alert companies to "abhorrent violent material" on their services, and if the companies fail to "expeditiously" remove it, they could be fined AU\$10.5 million (US\$7.7 million) or 10 percent of their annual revenue. Individuals may be fined AU\$2.1 million (US\$1.5 million) or imprisoned for up to three years. The law also penalizes companies that fail to notify the Australian Federal Police (AFP) of material depicting "abhorrent violent conduct" occurring in Australia within a reasonable time after they become aware of it. These penalties are subject to appeal. Critics have expressed concern that the new legislation could unreasonably place responsibility on executives and employees for content posted by users, in an industry that is already grappling with the challenges of reviewing the vast amounts of uploaded content.[5](#) Critics also expressed fear that the broad definition of "abhorrent violent material" and the haste with which companies must remove it may lead to disproportionate restrictions.[6](#)

Australia's copyright laws continue to evolve in response to the proliferation of copyright-infringing material online. In December 2018, the Copyright Act was amended to broaden its provisions, for example by allowing blocking injunctions to be extended from sites hosting the material to search-engine providers. In practice, the amendment requires search engines to take reasonable steps to block search results for sites that are subject to blocking injunctions.[7](#) The amendment also allows existing blocking injunctions to be extended to "new domain names associated with the blocked online location" without a new court order.[8](#)

Section 313(3) of the 1997 Telecommunications Act allows government agencies to block illegal online services. The application of the law proved controversial in 2013, when the Australian Securities and Investment Commission (ASIC) used Section 313(3) to ask ISPs to take down a fraudulent website. Several legitimate websites were blocked because their internet protocol (IP) addresses were included in the request.[9](#) While those websites were swiftly restored, the matter led to a formal review of Section 313(3) in 2015.[10](#) In response to recommendations produced by

the review, the Department of Communications and the Arts published new guidelines on the use of the provision in 2017. The guidelines provide “good practice measures” for agencies to follow, including obtaining authorization from the agency head before disrupting online services, limiting disruptions to instances of serious offenses or national security threats, providing information to the public on uses of Section 313(3), and ensuring that the agency possesses appropriate technical expertise.<sup>11</sup>

Copyright holders may apply to the Federal Court to request that copyright-infringing websites and services that are located overseas be blocked by Australian ISPs under the Section 115A of the Copyright Amendment (Online Infringement) Act of 2015.<sup>12</sup> When making a decision, the court must take into consideration whether the overseas site has a primary purpose of facilitating copyright infringement, whether the response is proportionate, and whether blocking is in the public interest.<sup>13</sup>

In early 2018, the Department of Communications and the Arts invited feedback on the implementation of the amendment. Most submissions indicated that the new legal regime was effective at reducing piracy and that the court process for injunctions was appropriate.<sup>14</sup> Submissions made by digital rights groups, including the Australian Digital Alliance, cautioned against any further amendments to the law that would extend its application beyond ISPs to other intermediaries, or any reduction in judicial oversight of the law’s application.<sup>15</sup>

- 1. <https://www.legislation.gov.au/Details/C2016C00607>
- 2. <https://slate.com/technology/2019/03/new-zealand-shooting-8chan-isps-bl...>
- 3. <https://www.gizmodo.com.au/2019/03/optus-telstra-block-sites-for-hostin...>
- 4. <https://www.legislation.gov.au/Details/C2019A00038>
- 5. ‘Australia passes social media law penalising platforms for violent content’ The Guardian, April 3 2019, <https://www.theguardian.com/media/2019/apr/04/australia-passes-social-m...>
- 6. <https://www.lawfareblog.com/australias-new-social-media-law-mess>
- 7. [http://www.copyright.org.au/acc\\_prod/ACC/Information\\_Sheets/Copyright I...](http://www.copyright.org.au/acc_prod/ACC/Information_Sheets/Copyright_I...); <https://www.communications.gov.au/what-we-do/copyright/copyright-reform>
- 8. [http://www.copyright.org.au/acc\\_prod/ACC/Information\\_Sheets/Copyright I...](http://www.copyright.org.au/acc_prod/ACC/Information_Sheets/Copyright_I...)
- 9. Renai LeMay, “Interpol filter scope creep: ASIC ordering unilateral website blocks,” Delimiter, May 15, 2013, <http://bit.ly/1OGxYoc>
- 10. 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,” <http://bit.ly/1zQYodS>

- [11](#). Department of Communications and the Arts, ‘Guidelines for the use of section 313(3) of the Telecommunications Act 1997 by government agencies for the lawful disruption of access to online services’ <https://www.communications.gov.au/documents/guidelines-use-section-3133...>
- [12](#). House of Representatives, Copyright Amendment (Online Infringement) Bill 2015, <http://bit.ly/1zEHKM6>
- [13](#). There are more listed considerations. See Copyright Act 1968, s 115A.
- [14](#). Department of Communications and the Arts, Review of the Copyright Online Infringement Amendment, <https://www.communications.gov.au/have-your-say/review-copyright-online...>
- [15](#). Department of Communications and the Arts, Review of the Copyright Online Infringement Amendment – Submission of the Australian Digital Alliance, <https://www.communications.gov.au/have-your-say/review-copyright-online..>

B4 0-4 pts

Do online journalists, commentators, and ordinary users practice self-censorship?

34

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.<sup>[1](#)</sup> Australian defamation laws are widely regarded as among the most favorable to plaintiffs in the world, and fear of defamation suits has driven some self-censorship among both the media and ordinary users ([see C2](#)). Legal defenses against defamation that are typically available in other democratic countries, such as the public-interest defense, are difficult to claim in practice, effectively inhibiting the publication of public-interest journalism when there is a risk of defamation accusations.<sup>[2](#)</sup> According to a survey of journalists published in 2019 by the Australian Media Entertainment and Arts Alliance, 80 percent of respondents reported that defamation laws made their jobs more difficult, with a quarter saying that stories they had written were not published due to fears of provoking defamation proceedings.<sup>[3](#)</sup>

In a separate problem, 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.<sup>4</sup> Some suppression orders are themselves excessively broad; both types can have a chilling effect on digital reporting. In June 2018, a judge in the state of Victoria imposed a global order suppressing reporting on the trial of Cardinal George Pell to mitigate the risk of a mistrial in a related legal proceeding involving Pell, who was ultimately convicted on the sex abuse charges in December of that year. Journalists criticized the suppression order for impeding reporting on a topic of high public importance. Though the order was lifted in February 2019, at least 30 journalists and other media professionals faced potential prosecution for alleged noncompliance with the order.<sup>5</sup>

- <sup>1</sup>. Jones v Toben (2002) FCA 1150 (17 September 2002), <http://bit.ly/1KSeqX0>
- <sup>2</sup>. 'Legal Frictions' The Walkley Magazine, July 24 2018, <https://medium.com/the-walkley-magazine/legal-frictions-96ee2b03b983>
- <sup>3</sup>. <https://www.meaa.org/download/the-publics-right-to-know-the-meaa-report...>
- <sup>4</sup>. Nick Title, "Open Justice - Contempt of Court" (Paper presentation, Media Law Conference Proceedings, Faculty of Law, University of Melbourne, February 2013)
- <sup>5</sup>. 'The Storm Around the Suppression Orders' The Law Society of NSW Journal, April 30 2019 <https://lsj.com.au/articles/the-storm-around-suppression-orders/>

B5 0-4 pts

Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?

44

The government does not control or manipulate online sources of information to advance any particular political interest. However, the media conglomerate News Corp Australia, which is controlled by Rupert Murdoch and is one of the leading players in the country's concentrated news media market, is regarded by some observers as editorially biased in favor of the conservative Liberal Party-National Party coalition government.<sup>1</sup>

The online portal of the publicly funded Australian Broadcasting Corporation (ABC) is a major source of news for Australians. Some members of the governing coalition have periodically called for the privatization of the ABC or cuts to its funding,<sup>2</sup> and commentators have characterized these proposals as a response to perceived left-leaning bias at the outlet. The persistent political pressure on the ABC has raised

concerns about the potential impact on its editorial independence.<sup>3</sup>

Australia's May 2019 federal elections featured a proliferation of online disinformation spread by domestic political parties. For example, the Liberal Party ran a targeted advertising campaign on Facebook that peddled false claims about the opposition Labor Party's plans for a "car tax."<sup>4</sup> The Liberal Party denied responsibility for a similar campaign on Facebook that included a fake press release outlining the Labor Party's plans for a so-called death tax.<sup>5</sup> In response to complaints regarding false information spread during the election campaign, Facebook representatives told Labor Party that the material would not be removed from the platform, but that it would be "demoted," resulting in fewer views.<sup>6</sup>

In March 2019, Facebook removed several accounts and pages "purporting to represent political communities in Australia" that originated in North Macedonia and Kosovo.<sup>7</sup> Ahead of the federal elections, Facebook temporarily banned non-Australians from taking out campaign ads in an effort to combat foreign interference in the polls.<sup>8</sup>

According to a 2019 report published by the University of Canberra, Australians' trust in news accessed through social media has fallen, with 49 percent of news consumers expressing distrust. Trust in the news media in general has also fallen, with 44 percent of respondents trusting news sources generally, a drop from the previous year. Sixty-two percent of Australians reported feeling concerned about fake news online. Nevertheless, many Australians access news primarily through social media, with 47 percent of those in their late teens or early 20s using such platforms as their main source of news. By contrast, only 3 percent of news consumers over the age of 73 reported social media as their main source of news.<sup>9</sup>

- <sup>1.</sup> "'New Low' for Journalism? Why News Corp's Partisan Campaign Coverage is Harmful to Democracy" The Conversation, May 9 2019, <https://theconversation.com/new-low-for-journalism-why-news-corps-parti...>
- <sup>2.</sup> 'Liberal Party council votes to sell off the ABC and move Australian embassy to Jerusalem' Sydney Morning Herald, June 16 2018 <https://www.smh.com.au/politics/federal/liberal-party-council-votes-to-...>
- <sup>3.</sup> Digital News Report 2018 - Australia, Reuters Institute for the Study of Journalism, <http://www.digitalnewsreport.org/survey/2018/australia-2018/>
- <sup>4.</sup> <https://www.theguardian.com/australia-news/2019/apr/10/liberal-party-fa...>
- <sup>5.</sup> <https://www.smh.com.au/federal-election-2019/bizarre-tricks-labor-hit-b...>
- <sup>6.</sup> <https://www.theguardian.com/australia-news/2019/jun/08/it-felt-like-a-b...>

- 7. <https://newsroom.fb.com/news/2019/03/cib-iran-russia-macedonia-kosovo/>
- 8. <https://www.reuters.com/article/us-australia-politics-facebook-idUSKCN1...>
- 9. <https://www.canberra.edu.au/research/faculty-research-centres/nmrc/digi...>

B6 0-3 pts

Are there economic or regulatory constraints that negatively affect users' ability to publish content online?

33

Users are generally free to publish content online without economic or regulatory constraints.

There are no limits on 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. The principle of net neutrality is not enshrined in any law or regulation. Some Australian ISPs and mobile service providers practice traffic shaping under what are known as fair-use policies: If a customer uses peer-to-peer file-sharing software, internet connectivity for those activities will be slowed in order to release bandwidth for other applications.<sup>1</sup>

- 1. Telstra, "Telstra Sustainability Report 2011," 19, <http://bit.ly/1nWJ6TC>

B7 0-4 pts

Does the online information landscape lack diversity? 44

The online landscape is fairly diverse, with content available on an array of topics. Australians have access to a broad selection of online news sources that convey uncensored political and social viewpoints.

However, the online news landscape is influenced by ownership concentration in the print media industry. News Corp accounts for more than half of newspaper circulation in Australia, while Nine (Fairfax Media) also holds a sizeable share. <sup>1</sup> News Corp's News.com.au is, according to some studies, the country's most-viewed news website, and the digital versions of News Corp newspapers such as the Australian are also popular.<sup>2</sup> Concerns about ownership concentration came to prominence ahead of the May 2019 federal elections. Consistent with News Corp's historically conservative political orientation, its outlets published content favorable to the incumbent coalition. Some commentators criticized the company's election

coverage as excessively one-sided and lacking in scrutiny of the coalition.<sup>3</sup> News Corp outlets have also been assailed for publishing content that is perceived to be supportive of white nationalism and prejudicial toward ethnic minorities.<sup>4</sup>

The ACCC reported in June 2019 that the rise of digital platforms has undermined the business model of most traditional journalism enterprises and had a particularly profound impact on smaller local news outlets. The commission found that this has resulted in a reduced volume of news production, raising concerns about broader effects on Australian society and democracy.<sup>5</sup>

Nevertheless, traditional and digital-only news outlets collectively continue to ensure a substantial level of diversity, and this is enhanced by other digital media such as blogs, Twitter feeds, Wikipedia pages, and Facebook groups.<sup>6</sup> 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 country's population.

- <sup>1.</sup> "A Very Australian Coup: Murdoch, Turnbull and the Power of News Corp" The Guardian, September 19 2018, <https://www.theguardian.com/media/2018/sep/20/very-australian-coup-murd...>
- <sup>2.</sup> "A Very Australian Coup: Murdoch, Turnbull and the Power of News Corp" The Guardian, September 19 2018, <https://www.theguardian.com/media/2018/sep/20/very-australian-coup-murd...>
- <sup>3.</sup> "'New Low' for Journalism? Why News Corp's Partisan Campaign Coverage is Harmful to Democracy" The Conversation, May 9 2019, <https://theconversation.com/new-low-for-journalism-why-news-corps-parti...>
- <sup>4.</sup> 'News Corp: Democracy's greatest threat' The Monthly, May 2019, <https://www.themonthly.com.au/issue/2019/may/1556632800/richard-cooke/n...>
- <sup>5.</sup> <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20...>
- <sup>6.</sup> 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://bit.ly/2sxJKfe>.

Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?

Australians use social media to petition the government and to mobilize for public protest without restrictions. For example, campaigns launched by GetUp!, an independent nonprofit advocacy group that campaigns on left-wing issues, garner significant engagement online. A YouTube video uploaded ahead of a 2017 postal survey on the possibility of legalizing same-sex marriage received more than 16 million views.<sup>1</sup> GetUp! utilizes online petitions to raise awareness and gather support for causes such as cracking down on corporate tax avoidance and corruption.<sup>2</sup>

Social media are sometimes used as a platform to scrutinize government policy. The Juice Media, a small local film company, uses Facebook and YouTube to post a highly popular video series called Honest Government Ads, which satirizes the government and covers topics such as Australia's climate, immigration, and foreign policies.<sup>3</sup>

In the lead-up to Australia Day in January 2017, some social media users mobilized around the #ChangeTheDate hashtag. Change the Date is an ongoing campaign to change the country's national day as part of an effort to recognize injustices suffered by the indigenous population.<sup>4</sup> More recently, Australians used online platforms to rally and petition the government to take action on climate issues.<sup>5</sup>

- <sup>1</sup>. <https://www.youtube.com/watch?v=TBd-UCwVAY>
- <sup>2</sup>. GetUp! <https://www.getup.org.au>
- <sup>3</sup>. <https://www.youtube.com/user/thejuicemedia/>
- <sup>4</sup>. Kevin Rennie, "Australia Day Ads Promoting Diversity Stir Controversy Before National Holiday," Global Voices, January 25, 2017, <http://bit.ly/2qxuSdT>
- <sup>5</sup>. [https://www.aph.gov.au/petition\\_sign?id=EN1041](https://www.aph.gov.au/petition_sign?id=EN1041)

## C Violations of User Rights

*While internet users in Australia are generally free to access and distribute materials online, expression is limited by a number of legal obstacles, such as broadly applied defamation laws and a lack of codified free speech guarantees. In addition, legislative changes in recent years have significantly increased the government's capacity for surveillance of ICTs, including a law adopted in December 2018 that empowered authorities to access encrypted data.*

C1 0-6 pts

Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, 56 and are they enforced by a judiciary that lacks independence?

Freedom of expression is not an explicitly protected constitutional or statutory right. The High Court has held that there is an implied freedom of political communication in the constitution, but this extends only to the limited context of political discourse during an election period.<sup>1</sup> Australians' rights to access online content and freely engage in online discussions are based less in law than on a shared understanding of the prerequisites for a fair and free society. The public benefits greatly from a culture of freedom of expression and freedom of information that is generally protected by an independent judiciary. The country is also a signatory to the International Covenant on Civil and Political Rights (ICCPR).

Australia has a free press, and journalists are able to report on most topics without restriction. However, ownership concentration limits the diversity of the news media landscape, both for online and traditional journalism ([see B7](#)). In addition, whistleblower laws, laws pertaining to defamation, and suppression orders can inhibit reporting ([see B4](#)).

- <sup>1</sup> Alana Maurushat and Renee Watt, "Australia's Internet Filtering Proposal in the International Context," *Internet Law Bulletin* 12, no. 2 (2009).

C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities?

24

Online activities that are protected under international human rights standards are

sometimes subject to criminal penalties in Australia, primarily through the country's defamation laws. The Sharing of Abhorrent Violent Material Act adopted in April 2019 introduced criminal code provisions that could also be applied to such activities ([see B3](#)).

Defamation law has been interpreted to favor plaintiffs and is governed by state-level legislation as well as common law principles.<sup>1</sup> However, there are several legal defenses against defamation claims, including those of truth, fair reporting on proceedings of public concern, and honest opinion. The majority of defamation cases between 2013 and 2017 involved online defamation, meaning ordinary social media users can find themselves exposed to lawsuits for their remarks.<sup>2</sup> The state government of New South Wales announced in June 2018 that it would champion a comprehensive overhaul of defamation law in response to the growing number of social media defamation cases.<sup>3</sup> A reform package is due to be completed and "parliament-ready" by June 2020.<sup>4</sup>

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 allegedly defamed person enjoys a reputation in Australia. This allows for the possibility of "libel tourism," in which foreign individuals file defamation cases in Australia against others based outside the country in order to take advantage of its favorable legal environment for plaintiffs. 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 involving a high risk that the defamation will continue.<sup>5</sup>

- <sup>1</sup>. Principles of online defamation stem from the High Court of Australia, *Dow Jones & Company Inc v. Joseph Gutnick* (2002) HCA, 56.
- <sup>2</sup>. Centre for Media Transition, 'Trends in Digital Defamation: Defendants, Plaintiffs, Platforms,' <https://www.uts.edu.au/sites/default/files/article/downloads/Trends%20i...>
- <sup>3</sup>. Sydney Morning Herald, 'NSW Pushes for Historic Overhaul of Defamation Laws' <https://www.smh.com.au/national/nsw/nsw-pushes-for-historic-overhaul-of...>
- <sup>4</sup>. New South Wales Government, National Defamation Law Reform, <https://www.justice.nsw.gov.au/Pages/media-news/news/2019/National-Defa...>

- [5.](#) Carolan v Fairfax Media Publications Pty Ltd (No 7).

C3 0-6 pts

Are individuals penalized for online activities? 56

There have been a number of high-profile lawsuits involving online defamation in recent years, with defendants including members of the professional press as well as ordinary social media users. Observers warn that the financial penalties involved are punitive could deter investigative reporting and free speech ([see B4](#)). In 2017, rulings favored the plaintiff in 43 percent of digital defamation cases, and courts awarded plaintiffs AU\$100,000 (US\$73,000) or more in seven suits.[1](#)

In a precedent-setting decision after the coverage period, a New South Wales Supreme Court judge ruled in June 2019 that media companies are liable for defamatory comments posted by third parties on their social media pages. The plaintiff, Dylan Voller, successfully argued that the media companies should have known of the significant risk of defamatory comments, and that they should have proactively monitored or hid the comments.[2](#)

In another recent case, actress Rebel Wilson was awarded AU\$600,000 (US\$440,000) in damages in June 2018 (reduced on appeal from an initial award of more than AU\$4.7 million), after a court found that online and print articles published by the magazine Women's Day had defamed Wilson. The articles in question suggested that the actress was a serial liar and untrustworthy.[3](#)

In a troubling 2017 case, the Supreme Court of New South Wales awarded a Tweed Heads shire councillor, Katie Milne, AU\$45,000 (US\$33,000) in damages after a local property developer told several journalists that she was not a fit and proper person to be a councillor. The defendant's comments were quoted in online publications. The judge found that although the plaintiff was voluntarily subjecting herself to the "slings and arrows" of public office, the defendant's statement was a "direct and fundamental" attack on her activities as a councillor and her right to remain one.[4](#)

- [1.](#) Centre for Media Transition, 'Trends in Digital Defamation: Defendants, Plaintiffs, Platforms,' <https://www.uts.edu.au/sites/default/files/article/downloads/Trends%20i...>
- [2.](#) <https://theconversation.com/can-you-be-liable-for-defamation-for-what-o...>; <https://www.abc.net.au/news/2019-06-24/court-finds-media-liable-for-fac...>
- [3.](#) Summary of BAUER MEDIA PTY LTD V WILSON [NO.2] [2018] VSCA 154,

Supreme Court of Victoria, <https://www.supremecourt.vic.gov.au/court-decisions/judgments-and-sente...>

- [4. Milne v Ell \[2017\] NSWSC 555 \(8 May 2017\)](#)  
<http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/nsw/NWSC/2017/555.h...>

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?

24

Individuals do not need to register to use the internet, and there are no restrictions on anonymous communications. However, verified identification information is required to purchase any prepaid mobile service.<sup>1</sup> Additional personal information must be submitted to a mobile service provider before a phone can be activated. All recorded information is stored while the service remains activated, and it may be accessed by law enforcement and emergency agencies with a valid warrant.<sup>2</sup>

In December 2018, Parliament passed the Telecommunications and Other Legislation Amendment (Assistance and Access) Act, which gives intelligence and security agencies the power to compel "communications providers" to change or break their own encryption technology upon request in order to facilitate access to user data (see C6).<sup>3</sup> The law prohibits assistance that would undermine encryption or security for users at large, but critics have noted that, in practice, it is difficult (and in some cases impossible) to enable authorities' access to one user's data without creating exploitable vulnerabilities that could affect others.<sup>4</sup>

- [1. https://privacyinternational.org/long-read/3018/timeline-sim-card-regis...](https://privacyinternational.org/long-read/3018/timeline-sim-card-regis...)
- [2. https://www.acma.gov.au/theACMA/id-checks-for-pre-paid-mobiles](https://www.acma.gov.au/theACMA/id-checks-for-pre-paid-mobiles)
- [3. https://www.bbc.com/news/world-australia-46463029](https://www.bbc.com/news/world-australia-46463029)
- [4. https://theconversation.com/the-governments-encryption-laws-finally-pas...](https://theconversation.com/the-governments-encryption-laws-finally-pas...)

C5 0-6 pts

Does state surveillance of internet activities infringe on users' right to privacy?

26

The government has expanded its surveillance and data-gathering capabilities in recent years. The Assistance and Access law adopted in December 2018 represents the latest such expansion. The Guardian reported in July 2019 that the AFP and

state police in New South Wales had issued five requests to access encrypted user data under the law in March, April, and May of that year.<sup>1</sup> The Australian Security Intelligence Organisation (ASIO), the country's domestic intelligence service, has also employed the new legislation. These requests are subject to judicial oversight.

While the Privacy Act 1988 (Cth) grants some privacy protections, it does not provide individuals with remedies for privacy breaches, regardless of whether the state or nonstate actors are responsible.<sup>2</sup> In 2017, Australia's Federal Court clarified that metadata do not qualify as personal information and are therefore not subject to statutory protections, further narrowing the scope of the Privacy Act.<sup>3</sup> Law enforcement agencies no longer require a warrant to access metadata under the 2015 Telecommunications (Interception and Access) Amendment (Data Retention) Act ([see C6](#)).

In 2014, Parliament enacted amendments to national security legislation that increased penalties for whistle-blowers and potentially allow intelligence agents to monitor an entire network with a single warrant. In particular, a new section (35P) added to the 1979 Australian Security Intelligence Organisation (ASIO) Act included provisions that threaten journalists and whistle-blowers with a 10-year prison term if they publish classified information related to special intelligence operations.<sup>4</sup> In response to a report prepared by the independent national security legislation monitor, Robert Gyles,<sup>5</sup> Section 35P was subsequently amended to offer some protections to journalists. The revised law distinguishes between disclosures made by "entrusted persons," which largely refers to ASIO employees, and those made by "outsiders," which would include journalists. The provisions for outsiders have a higher threshold of harm, applying only when disclosure would endanger the health or safety of another person or prejudice a special intelligence operation.<sup>6</sup> Other worrying amendments to the ASIO Act included changes to the scope of warrants; notably, the definition of "computer" was broadened to allow authorities to access data on multiple networked computers with a single warrant.

The incorporation of mass surveillance into ordinary policing has emerged as a new concern. An ABC investigation revealed that Queensland police used facial-recognition technology at the 2018 Commonwealth Games for general policing, as opposed to “high priority” targets, even though Queensland law only allows mass surveillance operations to identify suspects of serious crimes. Civil liberties advocates, who denounced the generalized use of the technology as “scope creep,” criticized Queensland police for failing to be transparent about the operation.<sup>7</sup>

Privacy concerns have also been raised in response to the launch of online databases and data-sharing initiatives. In 2017, the government announced the creation of a national facial biometric database that would make driver’s-license photographs and other images of citizens available across government departments. Critics characterized the move as a serious privacy violation to which citizens did not consent when they originally provided their photographs.<sup>8</sup>

Another initiative facing significant criticism from privacy groups, as well as parts of the medical community, is the government’s My Health Record, a database system created under a 2012 law that automatically generates a digital summary of citizens’ key health information. Amendments were enacted in December 2018 to address privacy concerns, requiring a court order before My Health Record data can be released to the police or government agencies.<sup>9</sup> However, concerns persist regarding the security of the data, especially because almost a million medical practitioners have access to the system, increasing the risk of breaches.<sup>10</sup>

- <sup>1.</sup> <https://www.theguardian.com/technology/2019/jul/10/new-encryption-power...>
- <sup>2.</sup> Rose Dlougatch, “Cyber Insecurity: Data Breaches, Remedies and the Enforcement of the Right to Privacy” Australian Journal of Administrative Law (2018) 25, <http://sites.thomsonreuters.com.au/journals/2019/02/18/australian-journ...>
- <sup>3.</sup> Privacy Commissioner v Telstra Corporation Limited
- <sup>4.</sup> National Security Legislation Amendment Act (No. 1) 2014, s 108.
- <sup>5.</sup> The Hon. Roger Gyles AO QC, “Report on the impact on journalists of section 35P of the ASIO Act,” October 2015, <http://bit.ly/29SPG7y>
- <sup>6.</sup> [https://www.aph.gov.au/Parliamentary\\_Business/Bills\\_Legislation/bd/bd16...](https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd16...)
- <sup>7.</sup> ‘Facial recognition system rollout was too rushed, Queensland police report reveals’ ABC News, May 5 2019, <https://www.abc.net.au/news/2019-05-06/australias-biggest-facial-recogn...>

- [8.](#) Bruce Baer Arnold, ‘:Let’s Face it, We’ll be no Safer with a national facial recognition database,’ The Conversation <https://theconversation.com/lets-face-it-well-be-no-safer-with-a-nation...>; <https://www.efa.org.au/2017/10/06/face-database-free-society/>
- [9.](#) [https://www.aph.gov.au/Parliamentary\\_Business/Bills\\_LEGislation/Bills\\_S...](https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_S...)
- [10.](#) ‘Security fears are still too high, so I'm opting out of My Health Record’ Australian Financial Review, August 6 2018, <https://www.afr.com/technology/web/security/security-fears-are-still-to...>

C6 0-6 pts

Are service providers and other technology companies required to aid the government in monitoring the communications of their users?

36

Technology companies’ involvement in state surveillance deepened during the coverage period, thanks largely to the Assistance and Access law adopted in December 2018. The law gives Australia’s intelligence and security agencies the power to compel “communications providers” to undermine their own encryption technology in order to obtain user data.<sup>1</sup> It allows these agencies to issue requests for encrypted data under a broad set of circumstances, including for the purpose of safeguarding the country’s national security, foreign relations, or economic well-being. Requests may also be issued for the purpose of enforcing criminal law.

Rights groups have criticised the new law’s broad reach, relative lack of oversight, and harsh penalties. Opponents have also raised concerns about its potentially stifling effect on the country’s technology sector, as local companies could be forced to create products that are less secure than those of their foreign competitors.<sup>2</sup> Companies that fail to cooperate could face fines of up to AU\$10 million (US\$7.3 million), while individuals could face prison time. The Department of Home Affairs maintains that the new law is necessary and that it will operate with sufficient oversight to prevent abuse. All requests for assistance are overseen by various Commonwealth bodies, depending on the requesting agency. Organizations subject to a request for assistance have the right to complain or appeal to the relevant oversight body for the requesting agency, and technical capability notices—which require the recipient to change or break their own encryption technology—must be issued by the attorney general and approved by the minister for communications.<sup>3</sup>

Law enforcement agencies with a lawful warrant may search and seize computers. They may also compel ISPs to intercept and store data from individuals suspected of committing a crime, as governed by the Telecommunications (Interception and Access) Act 1979 (TIAA). 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.<sup>4</sup> Unlawful collection of a communication and disclosure of its content can draw both civil and criminal sanctions.<sup>5</sup> 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.<sup>6</sup>

The 2015 Telecommunications (Interception and Access) Amendment (Data Retention) Act requires telecommunication companies to store two years' worth of customer metadata.<sup>7</sup> 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.<sup>8</sup> That month, the government confirmed that metadata would not be available for use in civil cases.<sup>9</sup>

The 2015 legislation added extra privacy protections for journalists, requiring security agencies to obtain a warrant before accessing journalists' metadata. However, incidents of unauthorized access have undermined faith in these safeguards.<sup>10</sup> In 2017, the 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 procedures.<sup>11</sup>

The data collection practices of technology firms have also come under scrutiny. Following revelations that Cambridge Analytica had improperly accessed the data of Facebook users, including more than 300,000 Australians, the Office of the Australian Information Commissioner (OAIC) launched an investigation into the matter in April 2018. The probe was expected to examine whether Facebook breached the Privacy Act 1988 (Cth) before determining appropriate remedial options.<sup>12</sup>

- <sup>1</sup>. <https://www.bbc.com/news/world-australia-46463029>
- <sup>2</sup>. Digital Rights Watch <https://digitalrightswatch.org.au/2019/05/10/digital-skills-investment-...>
- <sup>3</sup>. The Department of Home Affairs <https://www.homeaffairs.gov.au/about->

[us/our-portfolios/national-securit...](#)

- [4.](#) 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, <http://bit.ly/1GAvajG>
- [5.](#) 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, <http://bit.ly/1GAvajG>
- [6.](#) 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)
- [7.](https://clfr.globalnetworkinitiative.org/country/australia/) <https://clfr.globalnetworkinitiative.org/country/australia/>
- [8.](#) "Metadata retention scheme deadline arrives," ABC News, April 13, 2017, <http://www.abc.net.au/news/2017-04-13/metadata-retention-scheme-deadlin...>; "Data retention laws start but information not for civil cases," ABC News, April 13, 2017, <http://www.abc.net.au/news/2017-04-13/data-retention-laws-start-but-inf...>
- [9.](#) <https://www.zdnet.com/article/brandis-rules-out-data-retention-in-civil...>
- [10.](#) Paul Farrell, "The AFP and me: how one of my asylum stories sparked a 200-page police investigation," The Guardian, 12 February 2016, <http://bit.ly/2fv0tnu>
- [11.](#) "AFP officer accessed journalist's call records in metadata breach," ABC News, April 28, 2017, <http://www.abc.net.au/news/2017-04-28/afp-officer-accessed-journalists-...>
- [12.](#) Office of the Australian Information Commissioner, 'Facebook and Cambridge Analytica' <https://www.oaic.gov.au/media-and-speeches/statements/facebook-and-camb...>

C7 0-5 pts

Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities?

55

Violence against online commentators is rare in Australia. Controversial figures are occasionally subject to intimidation and death threats.

In a widely criticized move, the AFP raided the offices of the ABC and the home of a journalist in June 2019, after the coverage period. The raids came in response to the broadcaster's publication in 2017 of the "Afghan Files," a series of stories based on leaked documents that focused on misconduct and unlawful killings by Australian soldiers in Afghanistan. The AFP presented a warrant before entering ABC premises and searched through files relating to the stories, which appeared on the ABC's website.<sup>1</sup>

In a separate June 2019 incident, the AFP raided the home of News Corp journalist Annika Smethurst in response to a story she wrote the previous year regarding leaked plans to expand the government's spying powers. The warrant gave the AFP permission to search Smethurst's home, computer, and phone as part of their investigation into the alleged publication of classified material.<sup>2</sup> As of August 2019, the authorities had not ruled out prosecuting Smethurst.<sup>3</sup>

The media industry and civil society denounced these raids as a disturbing threat to press freedom that effectively undermined reporting on national security and defense matters.<sup>4</sup>

- 1. <https://www.abc.net.au/news/2019-06-05/abc-raided-by-australian-federal...>
- 2. <https://www.theguardian.com/australia-news/2019/jun/04/federal-police-r...>
- 3. <https://www.theguardian.com/australia-news/2019/aug/14/afp-wont-rule-ou...>
- 4. <https://www.abc.net.au/news/2019-06-05/abc-raided-by-australian-federal...>

C8 0-3 pts

Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack? 13

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

In February 2019, the government announced that the computer networks of Parliament and major political parties, including the Labor, Liberal, and National Parties, had been subjected to malicious activity.<sup>1</sup> The incident was blamed on a

"sophisticated state actor," which Prime Minister Scott Morrison declined to name.<sup>2</sup> Public suspicion fell on China, but the Chinese government dismissed the notion as "baseless."<sup>3</sup> In September 2019, after the coverage period, Australian intelligence reportedly came to the conclusion that China's Ministry of State Security was behind the attack.<sup>4</sup>

A large number of Australian users were likely affected by a breach at the international hotel company Marriott, which was revealed following a September 2018 investigation. Sensitive user information was compromised, including names, addresses, passport numbers, and other details. The breach has been attributed to Chinese intelligence services.<sup>5</sup>

In July 2018, hackers based in China breached the Australian National University's computer systems.<sup>6</sup> In May 2019, the university's systems were breached again, also by hackers based in China, resulting in the theft of 200,000 people's personal data.<sup>7</sup>

In June 2018, PageUp, an online platform used in the recruitment and hiring process by major Australian employers including Telstra, the Reserve Bank of Australia, the Commonwealth Bank, and the Attorney-General's Department, reported a breach in its network. The personal information of job applicants, staff members, and others may have been accessed by an unauthorized third party as a result of the breach. Thousands of users were advised to change their passwords promptly and remain vigilant for any potential misuse of their personal information.<sup>8</sup>

The Australian Cyber Security Center (ACSC) reported in April 2018 that about 400 Australian businesses had been targeted in the previous year by cyberattacks that were believed to have been initiated by the Russian government. Observers have speculated that the purpose of the intrusions may have been to prepare for more disruptive future attacks, though Cyber Security Minister Angus Taylor said that no data had been stolen.<sup>9</sup>

A notifiable data breach scheme came into effect in February 2018, requiring businesses and government organizations to notify users if their information was compromised in a data breach and that the breach could result in serious harm to the users.<sup>10</sup> The OAIC reported in March 2019 that, in the scheme's first year of operation, 964 data breaches were reported. The majority of reported incidents involved malicious or criminal acts, and the finance and health industries were the

most widely affected.<sup>11</sup>

- 1. 'ACSC detects malicious activity targeting political party networks' Australian Cyber Security Centre, <https://www.cyber.gov.au/news/parliament-house-network-compromise>
- 2. <https://www.nytimes.com/2019/02/18/world/australia/parliament-hack-stat...>
- 3. <https://www.theguardian.com/australia-news/2019/feb/19/china-rejects-au...>
- 4. <https://www.reuters.com/article/us-australia-china-cyber-exclusive/excl...>
- 5. 'Marriott, Starwood hit by security incident' Australian Cyber Security Centre, <https://www.cyber.gov.au/news/marriott-statement>; 'Did Marriott bloat Australia's official data breach numbers?' ITnews, May 13 2019, <https://www.itnews.com.au/news/did-marriott-bloat-australias-official-d...>
- 6. <https://www.smh.com.au/politics/federal/chinese-hackers-breach-anu-putt...>
- 7. <https://www.theguardian.com/australia-news/2019/jun/06/china-behind-mas...>
- 8. 'Bank details, TFNs, personal details of job applicants potentially compromised in major PageUp data breach' ABC News, 7 June 2018; Office of the Australian Information Commissioner, Joint Statement on the PageUp Limited Data Incident, 18 June 2018, <https://www.oaic.gov.au/media-and-speeches/statements/joint-statement-o...>
- 9. 'Russian hacking: Up to 400 Australian companies caught up in cyber attacks blamed on Moscow', ABC News <http://www.abc.net.au/news/2018-04-17/australians-caught-up-in-cyber-at...>
- 10. Privacy Act 1988 (Cth) Part IIIC
- 11. <https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-da...>



## Country Facts

- 

### **Freedom in the World Status**

Free

- 

### **Networks Restricted**

No

- 

### **Social Media Blocked**

No

- 

### **Websites Blocked**

No

- 

### **Pro-government Commentators**

No

- 

### **Users Arrested**

No

## **Previous Reports**

- [2018 Report](#)