FREEDOM ON THE NET 2018

Australia

FREE

79 /100

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

LAST YEAR'S SCORE & STATUS

79 /100 **Free**

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

Key Developments, June 1, 2017 - May 31, 2018

- In October 2017, the Supreme Court of New South Wales issued a global injunction requiring Twitter to remove posts and accounts associated with a user that had disseminated confidential information about the plaintiff in the case (see Content Removal).
- In the run-up to a vote to legalize same-sex marriage, social media became a battleground for fierce discussions and campaigning (See Media, Diversity, and Content Manipulation).
- The government drafted legislation to facilitate law enforcement access to encrypted communications (see Surveillance, Privacy, and Anonymity).

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 the 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 subjected 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. In mid-2018, the announcement of proposed legislation to compel technology companies to assist law enforcement in accessing encrypted data raised concerns among digital rights groups.

A. Obstacles to Access

There are few obstacles to internet access in Australia. Services continue to improve in remote and rural areas throughout the country, 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 enjoys a high internet penetration rate, with 86 percent of households having access to the internet. [1] This rate is expected to steadily increase with the implementation of the National Broadband Network (NBN), which includes expanded wireless, fiber to the node, and satellite services in rural communities. Australians predominantly access the internet through desktop or laptop computers and smartphones. [2]

Australians have a number of internet connection options, including DSL, mobile, fixed wireless, cable, satellite, fiber, and dial-up. [3] As of December 2017, almost all of the country's internet connections were broadband, while dial-up connections were virtually non-existent. [4] Telecommunications services are becoming cheaper in Australia, with the Australian Competition and Consumer Commission reporting in 2017 a 9.4 percent decrease in the annual price of a fixed broadband connection and a 6.7 percent decrease in the annual price for a wireless broadband connection. [5] By December 2017, the number of internet subscribers increased to 14.2 million. [6]

Once fully implemented, the NBN is expected to make high-speed broadband available to Australians in remote and rural areas. [7]

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 internet speeds, and high public cost have increasingly fueled criticisms of the project. As more homes and businesses connected to the NBN over the past year, complaints about speed and service have surged. [8] The federal government has implemented a program monitoring NBN speeds to verify that advertised speeds are accurate. [9] The NBN's completion date has been pushed back to 2020. [10]

Roughly 60 percent of all Australians have access to broadband speeds of 24 Mbps – 100 Mbps. [11] The Speedtest Global Index ranked Australia 52nd in the world for fixed broadband internet speed in August 2018. [12]

As of December 2017, the Australian Bureau of Statistics reported that there were 26.7 million mobile phone subscribers. [13] Fourth generation (4G) mobile services have driven recent growth, with all networks expanding coverage and the range of services available. [14] The Australian Communications and Media Authority (ACMA) is due to commence auctioning 5G spectrum to Australian telecommunications providers later in 2018. [15]

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. [16] Major internet service providers (ISPs) such as Telstra offer financial assistance to help low-income families connect to the internet. [17]

A digital divide persists between rural and urban areas, though it is narrowing. According to a 2018 Australian Bureau of Statistics report, 77 percent of households in regional areas have access to the internet compared to 88 percent of households in major cities. [18] In general, indigenous people and people with disabilities tend to have lower levels of internet access and digital literacy. [19]

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. [20] (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. [21]) However, the study did not assess internet use through mobile devices. [22] Telstra has committed to increasing coverage in rural areas, having invested in boosting its 4G service. [23]

Gender is not a barrier to accessing the internet, with approximately 85 percent of both men and women in urban areas accessing the internet in 2015. [24] In rural areas, 84 percent of women accessed the internet in the same period compared to 72 percent of men.

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 uses peer-to-peer file sharing software, internet connectivity for those activities will be slowed in order to release bandwidth for other applications. [25]

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. [26]

ICT Market

Australia hosts a competitive market for internet access, with 63 providers as of December 2015, including 10 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). [27] Telstra continues to dominate the fixed broadband and wireless broadband markets. [28]

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. [29] 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). [30]

As of 2017, Telstra continued leading the mobile market with a 43 percent market share, followed by Optus with 28 percent and VHA with 18 percent. [31]

Regulatory Bodies

The Australian Communications and Media Authority (ACMA) is the primary regulator for the internet and mobile telephony. [32] 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. [33] The industry's involvement consists of developing industry standards and codes of practice. [34] There are over 30 self-regulatory codes that govern and regulate Australian information and communication technologies (ICTs). ACMA approves self-regulatory codes produced by the Communications Alliance, Australia's main telecommunications industry body. [35]

Small businesses and residential customers may file complaints about internet, telephone, and mobile phone services with the Telecommunications Industry Ombudsman (TIO), [36] 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. [37]

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. [38] While the affected websites were swiftly restored, the matter led to a formal review of section 313(3) in 2015. [39] In response to recommendations produced by the review, the Department of Communications and the Arts published new guidelines on the use of section 313(3) in June 2017. The guidelines provide a number of "good practice measures" for agencies to follow, including obtaining authorization from the agency head before disrupting online services, limiting disruptions to instances of serious offences or national security threats, providing information to the public on uses of section 313(3), and ensuring that the agency possesses appropriate technical expertise. [40]

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.

[41] 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. [42] Popular websites that frequently host copyright infringing material, including Pirate Bay and Kickass Torrents, were blocked in two recent Federal Court judgments. [43] 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 in reducing piracy and that the court process for injunctions was appropriate. [44] Submissions made by digital rights groups, including the Australian Digital Alliance, cautioned against any further amendments to the law which would extend its application beyond ISPs to other intermediaries or any reduction in judicial oversight over the application of the law. [45]

In a recent positive development, Australian Parliament introduced new provisions into the Copyright Act in 2017 which relax copyright restrictions to facilitate accessibility for people with disabilities. The new provisions permit people with disabilities and organizations that assist people with disabilities to copy materials in order to convert them into accessible formats such as braille. [46]

Content Removal

Recent cases involving Google's search results and auto-complete predictions have sought to clarify how defamation laws are applied to such content online. In a recent 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 October 2017, the Supreme Court of New South Wales issued a global injunction against Twitter, in relation to a series of Tweets published by an anonymous user revealing confidential information about the plaintiff, company "X". Justice Pembroke ruled that the court possessed the necessary jurisdiction to grant an injunction against Twitter and ordered that Twitter be restrained from allowing the future publication of the offending material as well as requiring the removal of any instances of the offending material and any accounts associated with the anonymous user. The court considered Twitter's response objecting to the plaintiff's requested orders, in which the company stated that it would not be feasible to proactively monitor user

content. However, the court held that Twitter failed to provide an adequate explanation of why it would be unable to proactively monitor the content in question, and proceeded instead on the assumption that Twitter must possess a content filtering mechanism. [47] Commentators have regarded the decision with some concern, noting that the heavy-handedness of the Supreme Court could validate regional neighbors', such as China's, online censorship practices. [48]

In June 2018, the High Court of Australia allowed an appeal brought by Milorad Trkulja against Google after a lower court dismissed the appellant's defamation proceedings in 2017. The appellant argued that the Google auto-complete 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 somehow linked to the criminal underworld. [49] The proceedings may next be brought in the Victorian Supreme Court. [50]

In an earlier decision by the Supreme Court of South Australia in October 2015, Google was found liable as a secondary publisher of defamatory content about the plaintiff published by third party websites. The defamatory 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. [51] Google was ordered to pay damages to the plaintiff. [52] 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. [53] The Court dismissed Google's appeal in October 2017. [54]

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. [55] 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. [56]

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. [57] 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. Around 60 percent of Australians access news online using a smartphone. [58]

Same-sex marriage was legalized in Australia in December 2017 following a postal survey conducted earlier in the year by the Australian Bureau of Statistics. In the lead up to the vote, social media became host to fierce discussion and campaigning. Activists from both the "yes" and "no" camps have condemned the tone of the rhetoric online and reported that they had been subjected 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." [59] 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. [60]

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 expired in November 2017 after the survey was completed. [61]

According to a report published in 2018 by the University of Canberra, Australians report low levels of trust in news accessed through social media, with only 24 percent of those surveyed trusting news on social media. In comparison, 50 percent of respondents trusted news sources generally. Relatedly, almost three-quarters of news consumers reported encountering fake news online, with poor journalism and politically or commercially fabricated stories comprising the most common encounters. [62]

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). [63] 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. [64]

Digital Activism

Australians use social media to petition the government and to mobilize for public protest. Following a "Women's March On Washington" in the United States to promote human rights and end bigotry, a Sydney march with similar aims of supporting women and minorities was organized through social media. [65] Earlier popular protests included rallying against the closure of aboriginal communities in Western Australia [66] and protests at the G20 Summit in Brisbane. [67]

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. [68] The women at the center of the case launched an online advocacy group "Sexual Violence Won't be Silenced" to rally support against Alchin, as well as lobby for law reform and for the allocation of proper training and resources in the fight against sexual abuse against women online. [69]

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. [70]

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. [71]

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. [72] The majority of defamation cases between 2013-2017 involved online defamation, meaning ordinary

social media users can find themselves within reach of the courts. [73] 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. [74] Trends in digital defamation litigation may change in coming years as the government of the state of New South Wales announced in June 2018 a forthcoming comprehensive overhaul of defamation law as a response to the growing number of social media defamation cases. [75]

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 enables 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. [76]

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 2017, rulings favored the plaintiff in 43 percent of digital defamation cases, and courts awarded plaintiffs AUD $100,000 or more in approximately seven suits. [77]

In a troubling 2017 case, the Supreme Court of New South Wales awarded a Tweed Heads Shire Councillor, Katie Milne, AUD $45,000 in damages after a local property developer told several journalists that Ms. Milne was not a fit and proper person to be a Councillor. The defendant's comments were subsequently quoted in online publications. The judge found that though the plaintiff was an elected representative

voluntarily subjecting herself to the 'slings and arrows' of public office, the defendant's statement was a 'direct and fundamental' attack on the plaintiff's activities as a Councillor and her right to remain one. [78]

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. [79]

There have been cases in the states of New South Wales and Victoria of individuals being sentenced to prison for publishing explicit photos of women without consent, known as "revenge porn" because it is typically carried out by former partners. [80] 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. [81]

Surveillance, Privacy, and Anonymity

Over the past few years, the Australian government has expanded its surveillance and data gathering capabilities. While the Privacy Act 1988 (Cth) provides some privacy protections, the law does not provide an explicit and enforceable right to privacy. Commonwealth, state and territory privacy law is not consistent, and privacy watchdogs charged with administering and overseeing privacy laws are typically under-resourced. [82] In 2017, the Federal Court of Australia handed down a judgment clarifying that metadata does not qualify as personal information and is therefore not subject to statutory protections, further narrowing the scope of protections provided by the Privacy Act 1988 (Cth). [83]

In the midst of renewed debate over encryption, proposed legislation to facilitate law enforcement access encrypted communications has raised concerns that such measures could entail backdoor access and weakened security on popular platforms. [84] In May 2018, Cyber Security Minister Angus Taylor reiterated calls for government

access to encrypted communications, identifying the issue as a top priority. [85] Reports later emerged in June 2018 that the government had drafted legislation that would force companies to facilitate access to encrypted user data for security agencies. [86] While the government claims that the law will not mandate so-called "back doors" and "systemic" weaknesses to encryption, the latest draft contains language that could require companies to build "back door" type features to access particular devices or services. [87]

Law enforcement agencies with a lawful warrant may search and seize computers and compel an ISP to intercept and store data from those suspected of committing a crime, as governed by the Telecommunications (Interception and Access) Act 1979 (TIAA). Call-charge records are regulated by the Telecommunications Act 1997 (TA). [88] 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. [89] Unlawful collection and disclosure of the content of a communication can draw both civil and criminal sanctions. [90] 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. [91]

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. [92] In a recent development to the Act in April 2017, the government confirmed metadata will be excluded from being used in civil cases. [93]

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. [94] 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. [95]

In October 2014, parliament enacted amendments to national security legislation that increases 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. [96] 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 ICCPR. [97] The government announced their intention to support the six recommendations included in Gyle's report to better protect journalists and their sources, [98] 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.

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. [99]

Privacy concerns over online databases and data-sharing initiatives rose during the past year. In October 2017, the government announced the creation of a national facial biometric database, sharing driver's license and other photographs of citizens across government departments. Commentators criticized the move as a serious privacy violation to which citizens did not consent when they originally provided their photographs. [100]

Another initiative facing significant criticism from privacy groups and parts of the medical community was the government's My Health Record, a database system that will automatically generate a digital summary of citizens' key health information, with an option to opt out before November 2018. As part of the recent amendments intended to address privacy concerns, a court order will be required before My Health Record data is released to the police or government agencies. However, concerns persist regarding the security of the data, especially as almost one million medical practitioners will have access to My Health Record data, increasing the risks of breaches. [101]

Prior data-sharing initiatives have also come under fire. In 2017, controversy arose over the government's data-matching activities between Centrelink, Australia's social security program, and the Australian Tax Office, which was conducted to identify welfare fraud. Utilizing an "Online Compliance Intervention" program, the government automated the data-matching process and letters were automatically generated and sent to Centrelink users identified as having been overpaid. However, the algorithm behind the program was crude and failed to account for income fluctuations, resulting in thousands of alarming and inaccurate debt notices sent to Centrelink users. [102] The "robo-debt" saga prompted a senate inquiry which was highly critical of the program, finding that it was deeply flawed and set up to fail. [103]

Data collection practices of tech giants have also come under renewed scrutiny. Following revelations that Cambridge Analytica had improperly accessed Facebook users' data, including the data of over 300,000 Australian users, the Office of the Australian Information Commissioner (OAIC) launched an investigation into the matter in April 2018. The OAIC will investigate whether Facebook breached the Privacy Act 1988 (Cth) before determining appropriate remedial options. [104]

Intimidation and Violence

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

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. A notifiable data breach scheme came into effect in February 2018, requiring that certain businesses and government organizations notify users if their data was compromised in a data breach incident that could result in serious harm to the user. [105]

Telecommunications giant Telstra reported that 60 percent of Australian businesses had been affected by a cyberattack in 2017, with phishing attacks and Business Email Compromise the most common types of attacks. [106]

The Australian Cyber Security Center reported in April 2018 that around 400 Australian businesses had been targeted in the previous year by cyberattacks believed to have originated from the Russian government. Observers have speculated that the purpose of the attacks may have been to launch future attacks, though Cyber Security Minister Angus Taylor said that no data had been compromised. [107]

In June 2018, PageUp, an online service organization used in the recruitment process by several 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. Personal information of job applicants, staff members, and referees was potentially accessed by an unauthorized third party as a result of the breach. Thousands of users were advised to urgently change their passwords and remain vigilant to any potential misuse of their personal information. [108]

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. [109] Another high-profile

global ransomware phenomenon, WannaCry, had relatively little impact in Australia, though a small number of businesses were affected. [110]

According to the Australian Cyber Security Centre, the Computer Emergency Response Team responded to 14,804 cyberattack incidents between 2015 and 2016. [111] Targets included businesses, non-governmental agencies, and the Australian government.

Footnotes

1. Household Use of Information Technology, Australian Bureau of Statistics, 2016-2017 http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/8146.0Main+Features12016...
2. Ibid.
3. ABS, "Internet Activity, Australia, December 2017: Type of Access Connection," April 3, 2018, http://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/8153.0December%2020...
4. Ibid.
5. Australian Competition and Consumer Commission 'Competition and price changes in telecommunications services in Australia 2016-17' https://www.accc.gov.au/system/files/Competition%20and%20price%20change....

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 2018

Other Years

2020

Be the first to know what's happening.

Join the Freedom House monthly newsletter

Email

Subscribe

ADDRESS

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

GENERAL INQUIRIES
info@freedomhouse.org

PRESS & MEDIA
press@freedomhouse.org

@2020 FreedomHouse