AUSTRALIA

	2009	2011
INTERNET FREEDOM STATUS	**n/a**	**Free**
Obstacles to Access	n/a	3
Limits on Content	n/a	6
Violations of User Rights	n/a	8
Total	**n/a**	**17**

POPULATION: 22 million
INTERNET PENETRATION 2009: 75 percent
WEB 2.0 APPLICATIONS BLOCKED: No
SUBSTANTIAL POLITICAL CENSORSHIP: No
BLOGGERS/ONLINE USERS ARRESTED: No
PRESS FREEDOM STATUS: Free

INTRODUCTION

Although Australia enjoys affordable, high-quality access to the internet and other digital media, recent amendments to surveillance legislation and proposals to implement censorship through directives to internet-service providers (ISPs) have raised concerns about privacy and freedom of expression.[1] Draft legislation was proposed in 2010 that would require ISPs to filter illicit content and retain data on users' online activities. However, following the election of a new government, as of December 2010, these plans had been put on hold.

In 1989, Australia's Research and Education Network (AARNet) made the first internet connection with a 56 kilobit per second satellite link between the University of Melbourne and the University of Hawaii.[2] Today, the same connection to the United States is 200,000 times faster, and with the development of the high-speed National Broadband Network (NBN), all Australians, including those in more remote areas, will soon enjoy connection speeds near 100 megabits per second.[3] There were over 9.1 million active

[1] For a comprehensive overview of the legislative history of censorship in Australia *see* Libertus.net, "Australia's Internet Censorship System," http://libertus.net/censor/netcensor.html, accessed June 2010. *See also* Australian Privacy Foundation, http://privacy.org.au, accessed June 2010.
[2] Australia's Research and Education Network (AARNet), "AARNet Salutes the 20th Anniversary of the Internet in Australia," news release, November 26, 2009, http://www.aarnet.edu.au/Article/NewsDetail.aspx?id=173; Roger Clarke, "A Brief History of the Internet in Australia," May 5, 2001, http://www.rogerclarke.com/II/OzIHist.html; Roger Clarke, "Origins and Nature of the Internet in Australia," January 29, 2004, http://www.rogerclarke.com/II/OzI04.html.
[3] Australian Government, Department of Broadband, Communications and the Digital Economy, "National Broadband Network," http://www.dbcde.gov.au/broadband/national_broadband_network, accessed June 2010.

internet subscribers in Australia at the end of 2009 and nearly 16 million internet users, a penetration rate of approximately 75 percent.[4]

OBSTACLES TO ACCESS

Access to the internet and other digital media in Australia is widespread, almost ubiquitous. Australians have a number of internet connection options, including ADSL, ADSL 2+, wireless, cable, satellite, and dial-up.[5] Wireless systems can reach 99 percent of the population, while satellite capabilities are able to reach 100 percent. The phasing out of dial-up continues, with nearly 90 percent of internet connections now provided through other means. Once implemented, the NBN will eliminate the need for any remaining dial-up connections and make high-speed broadband available to Australians in remote and rural areas.[6]

In 2008, approximately 73 percent of people aged 14 and over lived in a household with an internet connection, while 58 percent lived in a household with a broadband connection.[7] These figures are expected to steadily increase to 100 percent with the implementation of the NBN. Although internet access is widely available in locations such as libraries, educational institutions, and internet cafes, Australians predominantly access the internet from home, work, and increasingly through mobile telephones. The majority of all age groups are using the internet, with the exception of those aged 65 and over.[8] Age is a significant indicator of internet use, with 100 percent of teenagers (aged 14 to 17) reporting that they have used the internet, 92 percent of them to a medium or heavy degree. By contrast, only 56 percent of those aged 65 and over have used the internet, and just 40 percent report heavy or medium usage.[9] Approximately 50 percent of Aboriginal and Torres Strait Islanders living in discrete indigenous communities (not major cities) have access to the internet with 36 percent having internet access in the home.[10]

---

[4] Australian Bureau of Statistics, "Internet Activity, Australia" (June, 2010), http://www.abs.gov.au/ausstats/abs@.nsf/mf/8153.0/ accessed December 30, 2010; International Telecommunications Union (ITU), "ICT Statistics 2009—Internet," http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False.

[5] Australian Communications and Media Authority (ACMA), *Communications Report, 2008–09* (Canberra: ACMA, 2009), http://www.acma.gov.au/webwr/_assets/main/lib311252/08-09_comms_report.pdf.

[6] Australian Government National Broadband Network, "NBN Key Questions and Answers" http://www.nbn.gov.au/content/nbn-key-questions-and-answers-faqs accessed June 2010.

[7] ACMA, *Communications Report, 2008–09*.

[8] ACMA, *Australia in the Digital Economy, Report 2: Online Participation* (Canberra: ACMA, 2009), http://www.acma.gov.au/WEB/STANDARD/pc=PC_311655.

[9] Ibid.

[10] Australian Bureau of Statistics, "Internet Access at Home" 2006, http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/4102.0Chapter10002008 accessed October 2010. For a

Australia has a mobile-phone penetration rate of 110 percent with many consumers using more than one SIM card or mobile phone.[11] In remote indigenous communities 63 percent of the population had taken up mobile-phone services in 2004.[12] However, not all indigenous communities have mobile-phone coverage such that the overall mobile-phone penetration rate in Aboriginal communities is unknown. Third-generation (3G) mobile services are the driving force behind the recent growth, with 12.28 million 3G mobile subscriptions operating as of June 2009.[13]

Internet access is affordable for most Australians. The government subsidizes satellite phones and internet connections for individuals and small businesses in remote and rural areas, where internet access is not comparable to that in metropolitan areas.[14]

Australia, like most other industrialized nations, hosts a competitive market for internet access, with 104 medium- to large-sized ISPs and another 585 small providers. Many of the latter are "virtual" maintaining only a retail presence and offering end users access through the network facilities of other companies.[15] ISPs are considered carriage-service providers under Australian law. As such they are required to obtain a license from the Australian Communications and Media Authority (ACMA) and submit to dispute resolution by the Telecommunications Industry Ombudsman (TIO). Australian ISPs are co-regulated under Schedule 7 of the 1992 Broadcasting Services Act (BSA), meaning there is a combination of regulation by the ACMA and self-regulation by the telecommunications industry.[16] The industry's involvement consists of the development of industry standards and codes of practice.

The government has adopted a strong policy of technical neutrality. There are no limits to the amount of bandwidth that ISPs can supply. While the government does not place restrictions on bandwidth, ISPs are free to adopt internal market practices on traffic shaping. Some Australian ISPs practice traffic shaping under what are known as fair-use policies. If a customer is a heavy peer-to-peer user, the internet connectivity for those activities will be slowed down to free bandwidth for other applications.[17] Advanced web applications like the social-networking sites Facebook and MySpace, the Skype voice-

comprehensive report on indigenous Internet use and access *see* ACMA, *Telecommunications in Remote Indigenous Communities* (Canberra: ACMA, 2008), page 48, http://www.acma.gov.au/WEB/STANDARD/pc=PC_311397 accessed June 2010.

[11] ACMA, *Communications Report, 2008-09*.

[12] ACMA, *Telecommunications in Remote Indigenous Communities*, page 30-32.

[13] ACMA, *Communications Report, 2008-09*.

[14] Rural Broadband, "Welcome," http://www.ruralbroadband.com.au, accessed June 2010.

[15] Australian Bureau of Statistics, "Internet Activity, Australia, Dec 2009," http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/8153.0Main+Features1Dec%202009?OpenDocument.

[16] Australian Communications and Media Authority Act 2005, http://www.austlii.edu.au/au/legis/cth/consol_act/acamaa2005453/; Broadcasting Services Act 1992, http://www.austlii.edu.au/au/legis/cth/consol_act/bsa1992214/; ACMA, "Service Provider Responsibilities," http://www.acma.gov.au/WEB/STANDARD/1001/pc=PC_90157, accessed June 2010.

[17] Vuze, "Bad ISPs," http://wiki.vuze.com/w/Bad_ISPs#Australia, accessed June 2010.

communications system, and the video-sharing site YouTube are neither restricted nor blocked in Australia.

The ACMA is the primary regulator for the internet and mobile telephony, and is responsible for enforcing Australia's anti-spam law.[18] Its oversight is generally viewed as fair and independent, though there are some transparency concerns with regard to classification of content. Small businesses and residential customers may file complaints about internet, telephone, and mobile-phone services with the Telecommunications Industry Ombudsman (TIO),[19] which operates as a free and independent dispute-resolution scheme.

LIMITS ON CONTENT

Australian law does not currently provide for mandatory blocking or filtering of websites, blogs, chat rooms, or platforms for peer-to-peer file sharing. Access to online content is far-reaching, and Australians are able to explore all facets of political and societal discourse, including information about human rights violations. Their ability to openly express dissatisfaction with politicians and to criticize government policies is not hindered by the authorities.[20]

However, there are two regimes that regulate internet content. Under one regime, material deemed by the ACMA to be "prohibited content" is subject to take-down notices. The relevant ISP is notified by the ACMA that it is hosting illicit content, and it is then required to take down the offending material.[21] Under the BSA, the following categories of online content are prohibited:

- Any online content that is classified Refused Classification (RC) by the Classification Board, including real depictions of actual sexual activity; child pornography; depictions of bestiality; material containing excessive violence or sexual violence; detailed instruction in crime, violence, or drug use; and material that advocates the commission of a terrorist act.

[18] ACMA, "The ACMA Overview," http://www.acma.gov.au/WEB/STANDARD/pc=ACMA_ORG_OVIEW, accessed June 2010;
ACMA, "How Regulation Works," http://www.acma.gov.au/WEB/STANDARD/pc=PUB_REG_ABOUT, accessed June 2010.

[19] Telecommunications Industry Ombudsman, http://www.tio.com.au, accessed June 2010.

[20] Chris Nash, "Freedom of the Press in Australia," Democratic Audit of Australia, November 19, 2003, http://democratic.audit.anu.edu.au/papers/20031119_nash_press_freed.pdf.

[21] Internet Society of Australia, "Who Is an Internet Content Host or an Internet Service Provider (and How Is the ABA Going to Notify Them?," http://www.isoc-au.org.au/Regulation/WhoisISP.html, accessed June 2010;
Stuart Corner, "EFA Fights ACMA Over 'Take-Down' Notice," iTWire, April 20, 2010, http://www.itwire.com/it-policy-news/regulation/38423-efa-fights-acma-over-take-down-notice; Internet Industry Association, "Guide for Internet Users," March 23, 2008, http://www.iia.net.au/index.php/initiatives/guide-for-users.html.

- Content that is classified R 18+ and not subject to a restricted access system that prevents access by children, including depictions of simulated sexual activity; material containing strong, realistic violence; and other material dealing with intense adult themes.
- Content that is classified MA 15+, provided by a mobile premium service or a service that provides audio or video content upon payment of a fee and that is not subject to a restricted access system, including material containing strong depictions of nudity, implied sexual activity, drug use, or violence; very frequent or very strong coarse language; and other material that is strong in impact.[22]

To date, this system for restricting access to videos, films, literature and similar material via take-down notices has not emerged as problematic in terms of any overflow to information of political or social consequence. In addition, the general disposition is to allow adults unfettered access to R 18+ materials while protecting children from exposure to inappropriate content.

Under the second regime, the ACMA may direct an ISP or content service provider to comply with the Code of Practice developed by the Australian Internet Industry Association (IIA) if the regulator decides that it is not already doing so. Failure to comply with such instructions may draw a maximum penalty of A$11,000 (US$10,800) per day. Other regulatory measures require ISPs to offer their customers a family-friendly filtering service.[23] This is known as voluntary filtering, as customers must select it as an option.

However, in recent years, the government has proposed implementing a mandatory filtering system run through ISPs.[24] Draft legislation was proposed under the Labor government led by Kevin Rudd, but was then put aside in the run-up to elections held in August 2010. Under the previously proposed draft, the list of sites to be blocked would initially focus on images of child abuse, particularly child pornography. The ACMA would have the responsibility of maintaining the blacklist, but the criteria for blocking sites remained nebulous. Under the latest proposal, the ACMA would blacklist any content classified as RC, and its early trials of internet filters used an initial list of over 1,300 sites, versions of which were leaked.[25] The list revealed that the overwhelming majority of

[22] ACMA, "Prohibited Online Content," http://www.acma.gov.au/WEB/STANDARD/pc=PC_90102, accessed June 2010.
[23] Internet Industry Association (IIA), *Internet Industry Code of Practice: Content Services Code for Industry Co-Regulation in the Area of Content Services (Pursuant to the Requirements of Schedule 7 of the Broadcasting Services Act 1992), Version 1.0*, 2008, http://www.iia.net.au/images/content_services_code_registration_version_1.0.pdf.
[24] Alana Maurushat, Renee Watt, "Australia's Internet Filtering Proposal in the International Context," *Internet Law Bulletin* 12, no. 2 (2009); ACMA, "Internet Service Provider Filtering," http://www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering.
[25] ACMA, "Internet Service Provider Filtering"; Wikileaks, "Australian Government Secret ACMA Internet Censorship Blacklist, 18 Mar 2009," http://mirror.wikileaks.info/wiki/Australian_government_secret_ACMA_internet_censorship_blacklist,_18_Mar_2009/, accessed February 2011.

websites hosted child pornography. However, there were a few notable exceptions of a gambling site, a euthanasia site, and a few pornography and fetish sites that did not host child pornography. The list, therefore, contained both banned content that it was designed to block and broader content that many would consider reasonable to remain accessible, fueling public fears that the system could be easily abused to expand censorship.

The proposed filtering system has been controversial in Australia as there are concerns of over-blocking, censorship of adult materials, scope creep, and impairment of telecommunication access speeds.[26] The federal elections in August 2010 saw the forming of a minority government with Julia Gillard of the Labor Party coming to power. While Gillard has voiced support for the filter in the media, the likelihood of any such proposal becoming law is slim due to the strong opposition to any such legislation by opposition parties.[27] Therefore, as of December 2010, the status of the initiative remained ambiguous and no internet filtering bill had been introduced in Parliament.

RC content, including many forms of adult pornography, is generally not unlawful to use, access, possess, or create in Australia merely by virtue of its RC status. Only material that is otherwise legislatively criminalized, such as material depicting child abuse and certain terrorism-related content, is unlawful. Moreover, Australia has no X 18+ or R 18+ category for video and computer games. This means that extremely violent video games beyond the MA 15+ classification level are necessarily categorised as RC.[28] The lack of a R +18 classification for video games has led to some peculiar results with games such as *Aliens vs Predators* initially given an RC classification which was later amended to M+ 15.[29] When a game is classified as RC often the developer will slightly modify the game to ensure an M+15 ranking.[30]

The currently existing classification system suffers from a lack of transparency, and there is no mechanism available for owners or creators to challenge the classification of RC content, which can be subject to take-down notices or possible blocking in the future by the proposed filter. Only the ISP or similar intermediary hosting the material may bring a challenge to the Administrative Appeals Tribunal (AAT). Australian content owners are not informed by the ACMA if it issues a take-down notice to their host.

---

[26] *See generally* Alana Maurushat and Renee Watt, Australia's Internet filter Proposal in the International Context, Internet Law Bulletin April 2009, page 18-25; and David Vaile and Renee Watt, "Inspecting the Despicable, Assessing the Unacceptable: Prohibited Packets and the Great Firewall of Canberra" (2009) University of New South Wales Law Review Series 35.

[27] The Sydney Morning Herald, "Internet Filter is Right: Gillard" October 12, 2010 http://news.smh.com.au/breaking-news-national/internet-filter-is-right-gillard-20101012-16hiz.html.

[28] Libertus.net, "Australia's Internet Censorship System," http://libertus.net/censor/netcensor.html; Wikileaks, "Australian Government Secret ACMA Internet Censorship Blacklist, 18 Mar 2009."

[29] Australian Government – Classification Review Board 2009, *Alien vs. Predator – Review Board Decision Reasons,* http://www.classification.gov.au/www/cob/rwpattach.nsf/VAP/%28C7C220BBE2D77410637AB17935C2BD2E%29~DecisionReasons-AliensvsPredator-Final-4January2010.pdf/$file/DecisionReasons-AliensvsPredator-Final-4January2010.pdf.

[30] See generally Chalk, OFLC reveals changes to Australian *Fallout 3*, August 13, 2008, http://www.escapistmagazine.com/news/view/85646-OFLC-Reveals-Changes-To-Australian-Fallout-3.

Journalists, commentators, and ordinary users are not subject to censorship so long as their content does not amount to defamation or breach criminal laws, such as those against hate speech or racial vilification.[31] Nevertheless, the need to avoid defamation has been a significant driver of self-censorship by both the media and ordinary users (see "Violations of Users' Rights").

Australians have access to a broad choice of online news sources that express diverse, uncensored political and social viewpoints. Individuals are able to use the internet and other technologies both as sources of information and as tools for mobilization.[32]

Digital media such as blogs, Twitter feeds, Wikipedia pages, and Facebook groups have been harnessed for a wide variety of purposes ranging from elections, to campaigns against government corporate activities, to a channel for safety-related alerts where urgent and immediate updates were required.[33] For instance, Google Maps was used in a creative endeavour to map out fire dissemination in the devastating 2009 wildfires that spread across the State of Victoria.[34]

VIOLATIONS OF USER RIGHTS

Australians' rights to access internet content and freely engage in online discussions are based less in law than 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.[35] The full range of human rights in Australia, unlike in other developed democratic nations, are not protected by a bill of rights or similar legislative instrument, though the country is a signatory to the International Covenant on Civil and Political Rights. Nonetheless, Australians benefit greatly from a culture of freedom of expression and freedom of information, further protected by an independent judiciary. However, the Australian press has consistently expressed concerns about a "culture of secrecy" that

[31] *Jones v. Toben* [2002] FCA 1150 (17 September 2002), http://www.austlii.edu.au/au/cases/cth/FCA/2002/1150.html, accessed June 2010.

[32] Re Lim, "Cronulla Riot: Confiscation of Mobile Phones, Invasion of Privacy and the Curbing of Free Speech," Act Now, March 15, 2006, http://www.actnow.com.au/Opinion/Cronulla_riot.aspx, accessed June 2010;
Les Kennedy, "Man in Court Over Cronulla Revenge SMS," *Sydney Morning Herald*, December 6, 2006, http://www.smh.com.au/news/national/man-in-court-over-cronulla-revenge-sms/2006/12/06/1165081008241.html.

[33] Digital media, for example, is readily used for political campaigning and political protest in Australia. *See* Terry Flew, "Not Yet the Internet Election: Online Media, Political Content and the 2007 Australian Federal Election" (2008) http://eprints.qut.edu.au/39366/1/c39366.pdf.

[34] Global Voices, "Australian Wildfire and Web Tools," February 9, 2009, http://globalvoicesonline.org/2009/02/09/australian-wildfires-and-web-tools/.

[35] Alana Maurushat, Renee Watt, "Australia's Internet Filtering Proposal in the International Context";
Australian Press Council, "Press Law in Australia," http://www.presscouncil.org.au/pcsite/fop/auspres.html#insult, accessed June 2010.

continues to inhibit reporting.[36] A 2007 report commissioned by Australia's Right to Know (ARTK), a coalition of media companies formed to examine free press issues, found that there were over 500 pieces of legislation containing "secrecy" provisions to restrict media publications. It also found barriers to accessing court information, little protection for whistleblowers, and inadequate shield laws to protect journalists.[37]

The Anti-Terrorism Act 2005 revived laws against sedition and unlawful association. The unlawful association provisions have been used widely since their enactment with the banning of several organizations perceived to be potentially dangerous in terms of intentions to commit violent acts.[38] The sedition provisions, however, have not been used. Further, insults against government institutions or officials would not fall within the sedition provisions.[39]

Australian defamation law has been interpreted liberally,[40] and is governed by legislation passed by the states as well as common-law principles. Civil actions over defamation are common and form the main impetus for self-censorship,[41] though a number of cases have established a constitutional defense when the publication of defamatory material involves political discussion.[42] In the online context, the lack of clarity on the responsibility of website operators to delete defamatory comments posted by other users has caused controversy. Court costs and stress associated with defending against suits under defamation laws have caused organizations to leave the country and blogs to shut down.[43] In one prominent case, the operator of the Australian discussion board ZGeek was named as a defendant in a defamation suit over comments posted on the forum that were critical of Greg Smith's conspiracy theory films.[44] Smith sued ZGeek in 2009 for over A$42 million (US$41 million) claiming that he did not land a lucrative film contract due to the comments. Although the Australian courts struck down the defamation suit, ZGeek announced plans to move its discussion forum to another jurisdiction.[45]

---

[36] David Rolph, Matt Vitins, and Judith Bannister, *Media Law: Cases, Materials and Commentaries* (South Melbourne: Oxford University Press, 2010), 44.

[37] Irene Moss, *Report of the Independent Audit into the State of Free Speech in Australia* (Surry Hills, New South Wales: Australia's Right to Know Coalition, 2007), http://www.smh.com.au/pdf/foIreport5.pdf.

[38] Andrew Lynch and George Williams, *What Price Security?* (UNSW Press, 2006) pages 41 to 59.

[39] See note above.

[40] Chris Nash, "Freedom of the Press in Australia," Democratic Audit of Australia, November 19, 2003, http://democratic.audit.anu.edu.au/papers/20031119_nash_press_freed.pdf. For more information generally on press freedom in Australia, see Reporters Without Borders, http://en.rsf.org/australie.html, accessed June 2010.

[41] Irene Moss, *Report of the Independent Audit*; Electronic Frontiers Australia, http://www.efa.org.au/category/defamation/, accessed June 2010.

[42] Human Rights Constitutional Rights, "Australian Defamation Law," http://www.hrcr.org/safrica/expression/defamation.html, accessed June 2010.

[43] See note 32 above; High Court of Australia, "Dow Jones & Company Inc v Joseph Gutnick," news release, December 10, 2002, http://www.hcourt.gov.au/media/dowjones.pdf.

[44] Asher Moses, "Online Forum Trolls Cost me Millions: Filmmaker" The Sydney Morning Herald, July 9, 2009, http://www.smh.com.au/technology/technology-news/online-forum-trolls-cost-me-millions-filmmaker-20090715-dl4t.html.

[45] EFA, "ZGeek Law Suit Struck Down" July 2009, http://www.efa.org.au/2009/07/15/zgeek-defamation-lawsuit-struck-out/.

Criminal defamation charges have also been filed over online content. Adelaide teenager Christopher Cross was convicted in November 2009 of criminal defamation for creating a Facebook group dedicated to criticizing a local police officer. Offensive comments, and some statements encouraging acts of violence against the constable, were posted on the page. Cross was convicted and placed on a two-year and A$500 (US$492) good behaviour bond. If Cross breaches the bond he could conceivably face up to three years in jail.[46] Under Australian law, a person may also bring a defamation case based on information posted by someone outside of Australia providing that the material is accessed in Australia and that the defamed person enjoyed a reputation in Australia.

Law enforcement agencies may search and seize computers, and compel an ISP to intercept and store data from those suspected of committing a crime. Such actions require a lawful warrant. The collection and monitoring of the content of a communication falls within the purview of the Telecommunications (Interception and Access) Act 1979 (TIAA). Call-charge records, however, are regulated by the Telecommunications Act 1997 (TA).[47] 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.[48] Unlawful collection and disclosure of the content of a communication can draw both civil and criminal sanctions.[49] The TIAA and TA expressly authorize a range of disclosures, including to specified law enforcement and tax agencies, all of which require a warrant.

ISPs are currently able to monitor their networks without a warrant for "network protection duties," such as curtailing malicious software and spam.[50] Australia has announced plans to accede to the Convention on Cybercrime.[51] Unlike many other countries that have already ratified the convention, Australia is expected to go beyond the treaty's terms in calling for greater monitoring of all internet communications by ISPs. Under the convention, an ISP is only required to monitor, intercept, and retain data when presented with a warrant, and only in conjunction with an active and ongoing criminal investigation. A document leaked in June 2010 from the Attorney General's Department describes a range of possible policy options under which Australian ISPs would be required to monitor, collect, and store information pertaining to all users' communications. This would be done without a warrant and enforced against all users regardless of whether there

[46] Nigel Hunt, "Teen Guilty of Facebook Slur," *Sunday Mail* (SA), November 22, 2009, http://www.adelaidenow.com.au/news/south-australia/teen-guilty-of-facebook-slur/story-e6frea83-1225801651074.
[47] Telecommunications Act 1997, Part 13, http://www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/.
[48] 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 http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/.
[49] Criminal offenses are outlined in Part 2-9 of the TIAA, while civil remedies are outlined in Part 2-10.
[50] 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, forthcoming.
[51] Convention on Cybercrime, Council of Europe, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG, accessed June 2010.

is a criminal investigation.[52] This compulsory data-retention policy, if enacted, could become a great threat to online freedom in Australia. The document is not official policy in Australia nor has it evolved into a concrete proposal or bill. As of December 2010, therefore, it was unclear whether such a policy would be realized in Australia.

Users do not need to register to use the internet, nor are there restrictions placed on anonymous communications. However, under a new election law in the state of South Australia that came into effect in January 2010, any individual posting a political comment in the run-up to local elections would be required to do so with their real name and address. The law applied to blogs and online news sites and non-compliance would draw a fine of up to A$1,250 (US$1,230). Following a public outcry, the state's attorney general and premier agreed to repeal the law.[53] Regarding mobile-phone users, verified identification information is required to purchase any prepaid mobile service. Additional personal information is required for 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 providing there is a valid warrant.[54]

Users of social-networking sites and similar applications have been threatened with physical violence and extralegal intimidation by other users, though not by state authorities. For example, a number of pages were established to memorialize Trinity Bates, a young girl who was abducted and brutally murdered in February 2010, and to call for violence against the accused killer. These sites were defaced by anonymous users who uploaded child pornography, and online and offline threats were then made against the suspected vandals.[55]

There have been a number of politically motivated cyberattacks, more specifically known as denial-of-service attacks (DoS) which have led to websites being inaccessible or flooded with substituted content for various lengths of time. The most well known attack is commonly referred to as Operation Titstorm. In February 2010, an internet group of activists known as Anonymous launched a DoS attack against the Australian Parliament House website in protest of the proposed internet filter.[56] The attack brought down Parliament's website for three days by bombarding it with pornographic images. It is unknown whether the Australian authorities have taken any measures to address politically

[52] Asher Moses, "Web Snooping Policy Shrouded in Secrecy," *The Age*, June 17, 2010, http://www.theage.com.au/technology/technology-news/web-snooping-policy-shrouded-in-secrecy-20100617-yi1u.html.
[53] Nate Anderson, "Internet Uprising Overturns Australian Censorship Law," Ars Technica, February 2, 2010, http://arstechnica.com/tech-policy/news/2010/02/internet-uprising-overturns-australian-censorship-law.ars; "South Australian Government Gags Internet Debate," News.com.au, February 2, 2010, http://www.news.com.au/technology/south-australian-state-government-gags-internet-debate/story-e6frfro0-1225825750956.
[54] ACMA, "Pre-paid Mobile Services—Consumer Information Provision Fact Sheet," http://www.acma.gov.au/WEB/STANDARD/pc=PC_9079, accessed June 2010.
[55] Emily Bourke and Kerrin Binnie, "Trinity Murder Inflames Facebook Debate," Australian Broadcasting Corporation (ABC), February 25, 2010, http://www.abc.net.au/news/stories/2010/02/25/2829635.htm.
[56] David Kravets, "Anonymous Unfurls 'Operation Titstorm'," *Wired Magazine*, February 10, 2010, http://www.wired.com/threatlevel/2010/02/anonymous-unfurls-operation-titstorm/#.

motivated DoS attacks.[57] More severe cyber attacks such as on the nation's critical infrastructure (such as electric grids, hospitals, banks) have occurred as well, though, to date, these have mostly been attacks on banking infrastructure for financial motives.[58]

[57] Websites typically cannot take preventative measures to ensure that they are not subject to a denial of service attack. Measures may only be taken once an attack has commenced to mitigate against damages.
[58] AusCERT Conference (2009), closed session invite only workshop on cybercrime, Chatham House Rules.