

# AUSTRALIA

	2011	2012
<b>INTERNET FREEDOM STATUS</b>	<b>Free</b>	<b>Free</b>
<b>Obstacles to Access (0-25)</b>	3	2
<b>Limits on Content (0-35)</b>	6	6
<b>Violations of User Rights (0-40)</b>	9	10
<b>Total (0-100)</b>	<b>18</b>	<b>18</b>

\* 0=most free, 100=least free

**POPULATION:** 22 million  
**INTERNET PENETRATION 2011:** 79 percent  
**WEB 2.0 APPLICATIONS BLOCKED:** No  
**NOTABLE POLITICAL CENSORSHIP:** No  
**BLOGGERS/ONLINE USERS ARRESTED:** No  
**PRESS FREEDOM STATUS:** Free

## INTRODUCTION

Australia enjoys affordable, high-quality access to the internet and other digital media. This quality of access improved in 2011 with the rollout of the National Broadband Network (NBN), a new communications network that aims to significantly improve broadband capacity and speed. Once fully implemented, the NBN will eliminate the need for any remaining dial-up connections and make high-speed broadband available in remote and rural areas.<sup>1</sup>

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. Nonetheless, privacy and freedom of expression concerns remain, particularly in the context of Australia's pending accession to the Convention on Cybercrime and the proposed Cybercrime Legislation Amendment Bill.<sup>2</sup> 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 internet service providers (ISPs).

<sup>1</sup> Australian Government National Broadband Network, "What is the NBN," accessed April 11, 2012, <http://www.nbn.gov.au/about-the-nbn/what-is-the-nbn/>.

<sup>2</sup> Cybercrime Legislation Amendment Bill 2011, Bills Digest no.31, 2011-12, accessed April 11, 2012, [http://www.aph.gov.au/Parliamentary\\_Business/Bills\\_Legislation/bd/bd1112a/12bd031](http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1112a/12bd031).

## OBSTACLES TO ACCESS

Access to the internet and other digital media is widespread, almost ubiquitous. Australians have a number of internet connection options, including ADSL, wireless, cable, satellite, and dial-up.<sup>3</sup> Wireless systems have the capacity to reach 99 percent of the population, while satellite capabilities are able to reach 100 percent. Dial-up has been phasing out, with nearly 90 percent of internet connections now provided through other means.

In 2011, the National Broadband Network (NBN) was launched to further expand high-speed internet access across the country. The NBN includes laying high-speed fiber-optic cable to connect homes and businesses in Australia and incorporate 93 percent of the country's population, with prioritization of the rollout to remote communities with either no broadband capacity or limited connection. The other 7 percent would connect to the internet by new satellite and fixed wireless technologies.<sup>4</sup> With the development of the high-speed National Broadband Network (NBN),<sup>5</sup> all Australians, including those in more remote areas, will soon enjoy peak connection at a minimum of 12 Mbps using a "nationwide network of fibre, fixed wireless and satellite technologies."<sup>6</sup>

In 2011, Australia had an internet penetration rate of 79 percent,<sup>7</sup> and between 2010 and 2011, additional one million households gained access to broadband internet, with 73 percent of households equipped with a broadband connection by December 2011.<sup>8</sup> These figures are expected to steadily increase 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.

People of all ages are using the internet, but the elderly population lags behind.<sup>9</sup> In fact, age is a significant indicator of internet use, with 69 percent of Australians between 18 and 24

<sup>3</sup> Australian Communications and Media Authority (ACMA), *Communications Report, 2010-2011* (Canberra: ACMA, 2011), accessed March 2012, [http://www.acma.gov.au/webwr/assets/main/lib410148/communications\\_report\\_2010-11.pdf](http://www.acma.gov.au/webwr/assets/main/lib410148/communications_report_2010-11.pdf).

<sup>4</sup> Nick Galvin, "A Nation on The Broadband Wagon," in the special report, *Update on the NBN*, The Sydney Morning Herald, April 23, 2012, <http://www.thenewspaperworks.com.au/files/dmfile/optus-nbn.pdf>.

<sup>5</sup> Australian Government, Department of Broadband, Communications and the Digital Economy, "National Broadband Network," accessed March 2012, [http://www.dbcde.gov.au/broadband/national\\_broadband\\_network](http://www.dbcde.gov.au/broadband/national_broadband_network).

<sup>6</sup> National Broadband Network Corporation, "Broadbanding Australia," accessed March 2012, [www.nbnco.com.au/assets/brochures/nbn-co-corporate-brochure.pdf](http://www.nbnco.com.au/assets/brochures/nbn-co-corporate-brochure.pdf).

<sup>7</sup> International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, <http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#>.

<sup>8</sup> Australian Bureau of Statistics, "Nearly three-quarters of Australian households now have broadband," media release, December 15, 2011, <http://www.abs.gov.au/AUSSTATS/abs@.nsf/Latestproducts/8146.0Media%20Release12010-11?opendocument&tabname=Summary&prodno=8146.0&issue=2010-11&num=&view=>, accessed March 1 2012.

<sup>9</sup> Australian Bureau of Statistics, "Household Use of Information Technology, Australia, 2010-11," December 2011.

years accessing the internet at home on a daily basis, and 75 percent of people 15 years or over reporting having used the internet in the past 12 months.<sup>10</sup> By contrast, only 31 percent of those 65 and over had used the internet during the same time period.<sup>11</sup> 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.<sup>12</sup>

Australia had a mobile phone penetration rate of 108 percent in 2011 with some consumers using more than one phone or SIM card.<sup>13</sup> Third-generation (3G) mobile services are the driving force behind the recent growth in usage.<sup>14</sup> The overall mobile phone penetration rate in Aboriginal communities is unknown, however, and not all indigenous communities have mobile phone coverage.

Australia, like most other industrialized nations, hosts a competitive market for internet access, with 97 medium to very large ISPs in June 2011,<sup>15</sup> as well as hundreds of small ISPs. Many of the latter are “virtual” ISPs, maintaining only a retail presence and offering end users access through the network facilities of other companies.<sup>16</sup> ISPs are considered carriage service providers (CSPs) under Australian law. As such, they are required to obtain a license from the Australian Communications and Media Authority (ACMA) and to be members of the Telecommunications Industry Ombudsman (TIO), an independent dispute resolution service. 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.<sup>17</sup> 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, and ISPs are free to adopt internal market practices on traffic-shaping. Some Australian ISPs practice traffic-shaping under what are

<sup>10</sup> Australian Bureau of Statistics, “ONLINE @ HOME,” June 2011, accessed March 2012, <http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/4102.0Main+Features50Jun+2011>.

<sup>11</sup> Ibid.

<sup>12</sup> Australian Bureau of Statistics, “Internet Access at Home,” 2008, accessed October 2010, <http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/4102.0Chapter10002008>. For a comprehensive report on indigenous Internet use and access, see: ACMA, *Telecommunications in Remote Indigenous Communities* (Canberra: ACMA, 2008), p 48, [http://www.acma.gov.au/WEB/STANDARD/pc=PC\\_311397](http://www.acma.gov.au/WEB/STANDARD/pc=PC_311397).

<sup>13</sup> International Telecommunication Union (ITU), “Mobile-cellular telephone subscriptions,” 2011, accessed July 13, 2012, <http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#>.

<sup>14</sup> Ibid.

<sup>15</sup> Australian Bureau of Statistics, “Internet Activity, Australia, June 2011.”

<sup>16</sup> Australian Bureau of Statistics, “Internet Activity, Australia, Dec 2009.”

<sup>17</sup> “Australian Communications and Media Authority Act 2005,” accessed June 2010, [http://www.austlii.edu.au/au/legis/cth/consol\\_act/acamaa2005453/](http://www.austlii.edu.au/au/legis/cth/consol_act/acamaa2005453/); “Broadcasting Services Act 1992,” accessed June 2010, [http://www.austlii.edu.au/au/legis/cth/consol\\_act/bsa1992214/](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](http://www.acma.gov.au/WEB/STANDARD/1001/pc=PC_90157).

known as fair-use policies. If a customer is a heavy peer-to-peer user, for example, internet connectivity for those activities are slowed down to free bandwidth for other applications.<sup>18</sup> Advanced web applications such as the social-networking sites Facebook and MySpace, the Skype voice-communications system, and the video-sharing site YouTube are neither restricted nor blocked in Australia.

## LIMITS ON CONTENT

Australian law does not provide for mandatory blocking or filtering of websites, blogs, chat rooms, or platforms for peer-to-peer file sharing. Users are able to access a wide range of information, and their ability to openly express dissatisfaction with politicians and criticize government policies is not hindered by the authorities.<sup>19</sup>

However, there are two systems in place that regulate internet content and place some restrictions on what can be viewed online. First, material deemed by the ACMA to be “prohibited content” is subject to take down notices. The ACMA notifies the relevant ISP that it is hosting illicit content and is then required to take down the offending material.<sup>20</sup> 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.
- ❖ 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

<sup>18</sup> “Bad ISPs,” VuzeWiki, accessed June 2010, [http://wiki.vuze.com/w/Bad\\_ISPs#Australia](http://wiki.vuze.com/w/Bad_ISPs#Australia).

<sup>19</sup> Chris Nash, “Freedom of the Press in Australia,” Democratic Audit of Australia, November 19, 2003, <http://apo.org.au/research/freedom-press-australia>.

<sup>20</sup> “Who Is an Internet Content Host or an Internet Service Provider (and How Is the ABA Going to Notify Them?)” Internet Society of Australia, accessed June 2010, <http://www.isoc-au.org.au/Regulation/WhoisISP.html>; 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>; “Guide for Internet Users,” Internet Industry Association, March 23, 2008, <http://www.ii.net.au/index.php/initiatives/guide-for-users.html>.

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.<sup>21</sup>

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 system, 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). Failure to comply with such instructions may draw a maximum penalty of AUD\$11,000 (US\$11,400) per day. Other regulatory measures require ISPs to offer their customers a family-friendly filtering service.<sup>22</sup> This is known as voluntary filtering, as customers must select it as an option.

Draft legislation on mandatory filtering was proposed under the Labour government led by Kevin Rudd and then put aside during the election in August 2010. There have been no indications by the current Labour government led by Julia Gillard as to whether draft legislation on the matter will be reintroduced in the immediate future, but statements have been made that the government has no intention to abandon the plan altogether.<sup>23</sup> The list of sites to be blocked would initially focus on images of child abuse, particularly child pornography.

The proposed filtering system has been controversial due to concerns of over-blocking, censorship of adult materials, scope creep, and impairment of telecommunication access speeds.<sup>24</sup> While Prime Minister 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.<sup>25</sup> In the interim, the three largest ISPs in Australia

---

<sup>21</sup> ACMA, "Prohibited Online Content," accessed June 2010, [http://www.acma.gov.au/WEB/STANDARD/pc=PC\\_90102](http://www.acma.gov.au/WEB/STANDARD/pc=PC_90102).

<sup>22</sup> 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.iaa.net.au/images/content\\_services\\_code\\_registration\\_version\\_1.0.pdf](http://www.iaa.net.au/images/content_services_code_registration_version_1.0.pdf).

<sup>23</sup> Alana Maurushat and Renee Watt, "Australia's Internet Filtering Proposal in the International Context," *Internet Law Bulletin* 12, no. 2 (2009); ACMA, "Internet Service Provider (ISP) Filtering," October 2011, [http://www.dbcde.gov.au/funding\\_and\\_programs/cybersafety\\_plan/internet\\_service\\_provider\\_isp\\_filtering](http://www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering).

<sup>24</sup> See generally, Alana Maurushat and Renee Watt, "Australia's Internet filter Proposal in the International Context," *Internet Law Bulletin* 12, no. 2 (2009), page 18-25; and David Vaile and Renee Watt, "Inspecting the Despicable, Assessing the Unacceptable: Prohibited Packets and the Great Firewall of Canberra," *University of New South Wales Law Review Series* 35 (2009).

<sup>25</sup> "Internet Filter is Right: Gillard," *The Sydney Morning Herald*, October 12, 2010, <http://news.smh.com.au/breaking-news-national/internet-filter-is-right-gillard-20101012-16hiz.html>.

(Telstra, Optus and Primus) voluntarily filter material listed as child abuse or child pornography.<sup>26</sup>

The many problems of classifying content in Australia came to light in the 2011 public inquiry and review of the current classification scheme by the Australian Law Reform Commission (ALRC). The ALRC released its final report in February 2012 entitled, “Classification-Content Regulations and Convergent Media,” which recommended the creation of a new single regulator of classification and content, among other key features.<sup>27</sup> The new national classification scheme will also emphasise eight guiding principles.<sup>28</sup> While the ALRC’s report announced sweeping reform to the classification and convergence of media content, it remains to be seen if the government will heed any of the recommendations.

Journalists, commentators, and ordinary users in Australia 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.<sup>29</sup> Nevertheless, the need to avoid defamation has been a significant driver of self-censorship by both the media and ordinary users (see “Violations of User Rights”).

Aside from restrictions on prohibited content, incitement to violence, racial vilification, and defamation, 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.<sup>30</sup> 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.<sup>31</sup> For instance, Google maps were used in a creative endeavor to map out fire dissemination in the devastating 2009 wildfires that spread across

<sup>26</sup> “Internet Service Provider (ISP) Filtering,” accessed April 23, 2012,

[http://www.dbcde.gov.au/funding\\_and\\_programs/cybersafety\\_plan/internet\\_service\\_provider\\_isp\\_filtering](http://www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering).

<sup>27</sup> For some of the key features of the ALRC’s new model, see: Australian Law Reform Commission, “Classification-Content Regulation and Convergent Media Final Report,” February 2012, p 24, accessed April 23, 2012, [http://www.alrc.gov.au/sites/default/files/pdfs/publications/final\\_report\\_118\\_for\\_web.pdf](http://www.alrc.gov.au/sites/default/files/pdfs/publications/final_report_118_for_web.pdf).

<sup>28</sup> See, *Ibid*, p 24-30.

<sup>29</sup> *Jones v. Toben* [2002] FCA 1150 (17 September 2002), <http://www.austlii.edu.au/au/cases/cth/FCA/2002/1150.html>.

<sup>30</sup> 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](http://www.actnow.com.au/Opinion/Cronulla_riot.aspx); 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>.

<sup>31</sup> 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/12611/1/12611.pdf>.

the State of Victoria.<sup>32</sup> In 2011, Twitter feeds were used to assist the mobilization of people in the Occupy Sydney and Occupy Brisbane movements.<sup>33</sup>

## VIOLATIONS OF USER RIGHTS

Australians' right to access internet content and freely engage in online discussions is 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.<sup>34</sup> The full range of human rights in Australia, unlike in most other developed democracies, is not protected by a bill of rights or similar legislative instrument, and the courts have less ground to strike down legislation that infringes on civil liberties. Nonetheless, Australians benefit greatly from a culture of freedom of expression and freedom of information, further protected by an independent judiciary. The country is also a signatory to the International Covenant on Civil and Political Rights (ICCPR).

Australian defamation law has been interpreted with a wide scope<sup>35</sup> and is governed by legislation passed by the states as well as common-law principles. A person may bring a defamation case based on information posted by someone outside of Australia provided that the material can be accessed in the country and the defamed person enjoys a reputation in Australia. Civil actions over defamation are common and form the main impetus for self-censorship,<sup>36</sup> though a number of cases have established a constitutional defense when the publication of defamatory material involves political discussion.<sup>37</sup> In one example in 2009, the operator of the Australian online discussion board ZGeek was named as a defendant in an AUD\$42 million (US\$43.5 million) defamation suit over comments posted on the forum,<sup>38</sup> but the case was later struck down by the courts.<sup>39</sup>

<sup>32</sup> John Liebhart, "Australian wildfires and web tools," Global Voices, February 9, 2009, <http://globalvoicesonline.org/2009/02/09/australian-wildfires-and-web-tools/>.

<sup>33</sup> The Occupy Sydney Twitter page is available at <http://twitter.com/occupySYDNEY>. The Occupy Brisbane Twitter page is also available at <http://twitter.com/OccupyBrisbane>.

<sup>34</sup> For a full analysis of freedom of expression in Australia, see: Alana Maurushat and Sophia Christou, "Waltzing Matilda or Advance Australia Fair: Fair dealings copyright exemptions with user-generated content," *Media & Arts Law Review*, March 2009.

<sup>35</sup> Chris Nash, "Freedom of the Press in Australia," Democratic Audit of Australia, November 19, 2003. For more information generally on press freedom in Australia, see: Reporters Without Borders, <http://en.rsf.org/australie.html>.

<sup>36</sup> Irene Moss, "Report of the Independent Audit into the State of Free Speech in Australia," Australia's Right to Know Coalition, October 31, 2011, [http://www.alliance.org.au/documents/071031\\_right\\_to\\_know\\_report.pdf](http://www.alliance.org.au/documents/071031_right_to_know_report.pdf).

<sup>37</sup> Human Rights Constitutional Rights, "Australian Defamation Law," accessed June 2010, <http://www.hrcr.org/safrica/expression/defamation.html>.

<sup>38</sup> Asher Moses, "Online Forum Trolls Cost me Millions: Filmmaker," Sydney Morning Herald, July 9, 2009, <http://www.smh.com.au/technology/technology-news/online-forum-trolls-cost-me-millions-filmmaker-20090715-dl4t.html>.

<sup>39</sup> "ZGeek Law Suit Struck Down," Electronic Frontiers Australia, July 15, 2009, <http://www.cfa.org.au/2009/07/15/zgeek-defamation-lawsuit-struck-out/>.

Criminal defamation charges have also been filed over online content. There have been a series of recent publicized defamation suits involving foreign companies such as Google, Yahoo, and Twitter. In October 2011 the Supreme Court of Queensland ordered Google Australia to release the details of the creators of websites that had published defamatory material about the author Jamie McIntyre.<sup>40</sup> In January 2012, the online music critic Joshua Meggitt instigated proceedings against Twitter in Australia for failing to remove a defamatory tweet about him.<sup>41</sup> In another case in April 2012, health researcher Dr. Janice Duffy sued Google for refusing to remove defamatory links to the U.S.-based consumer complaint website, Ripoff Report, from the Google search engine.<sup>42</sup>

Law enforcement agencies may search and seize computers and compel an ISP to intercept and store data from those suspected of committing a crime, but such actions require a lawful warrant. The collection and monitoring of communications fall within the purview of the Telecommunications (Interception and Access) Act 1979 (TIAA). Call-charge records, however, are regulated by the Telecommunications Act 1997 (TA).<sup>43</sup> It is prohibited for ISPs and similar entities, acting on their own, to monitor and disclose the content of communications without the customer's consent.<sup>44</sup> Unlawful collection and disclosure of the content of a communication can draw both civil and criminal sanctions.<sup>45</sup> 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.<sup>46</sup> Pending Australia's accession to the Convention on Cybercrime and adoption of the Cybercrime Legislation Amendment Bill 2011,<sup>47</sup> ISPs will be required to perform wider monitoring functions. Unlike many other countries that have already ratified the convention, Australia is expected to go beyond the

---

<sup>40</sup> Alison Sandy and Alex Dickinson, “Supreme Court Orders Google Australia to Release Details of Creators of Website,” News Australia, October 7, 2011, <http://jamiemcintyre.com/jamie-mcintyre-winning-battle-supremem-court-orders-google-australia-release-details-creators-defamatory-website/>.

<sup>41</sup> “Australian Joshua Meggitt Sues Twitter,” Socialite Media, February 20, 2012, <http://socialitemedia.com.au/australian-joshua-meggitt-sues-twitter/824/>.

<sup>42</sup> Rachel Wells, “Google in the Gun as Cyber Victims Fight Back,” Sydney Morning Herald, April 2, 2012, <http://www.smh.com.au/technology-news/google-in-the-gun-as-cyber-hate-victims-fight-back-20120401-1w6nf.html#ixzz1rmmmBLSx>.

<sup>43</sup> Telecommunications Act 1997, Part 13, accessed June 2010, [http://www.austlii.edu.au/au/legis/cth/consol\\_act/ta1997214/](http://www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/).

<sup>44</sup> 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/](http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/).

<sup>45</sup> Criminal offenses are outlined in Part 2-9 of the TIAA, while civil remedies are outlined in Part 2-10.

<sup>46</sup> 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.

<sup>47</sup> Cybercrime Legislation Amendment Bill 2011, Bills Digest no. 31, 2011-12, accessed April 11, 2012, [http://www.aph.gov.au/Parliamentary\\_Business/Bills\\_Legislation/bd/bd1112a/12bd031](http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1112a/12bd031).

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 of types of crimes listed in the Convention: fraud and forgery; copyright; unauthorized access, modification and interference to data or data system (computer, network); and child pornography provisions.

Under the proposed bill, timely preservation of evidence that might otherwise be lost may be obtained without a warrant. Preservation notices are issued by the Australian Federal Police (AFP) and are available for both domestic and international investigations. Carriage service providers (CSP in the legislation but commonly interchanged with ISP) must preserve stored communications of a target(s) for up to 90 days, depending on the type of preservation notice received from the AFP. A foreign country may also send a request to the AFP, who would then make a request to the Australian CSP. It is important to note, however, that preservation notices compel a carriage service provider merely to store information and that communications may only be disclosed when a valid Australian warrant has been issued.

Public input into Australia's accession to the Convention was sought in the form of a Cybercrime Inquiry. Many submissions to the inquiry expressed concern over a lack of safeguards, the privacy invasiveness of the proposed provisions,<sup>48</sup> and the overly broad scope of cooperation with foreign parties extending beyond the requirements of the Convention.<sup>49</sup> For example, the Convention only requires mutual cooperation between countries for preservation notices and real time evidence collection in the context of four areas: fraud and forgery; child pornography; copyright infringement; and unauthorized access, modification or interference with data, data systems or a computer. The Australian proposal does not limit mutual cooperation to the crimes specified in the Convention but potentially opens the door to any type of crime.

Presently, ISPs are required by law to have real time interception capabilities,<sup>50</sup> generally to be used for gathering evidence in connection with serious offenses such as murder, terrorism, and child pornography.<sup>51</sup> Under the proposed Cybercrime Legislation Amendment Bill, such real time evidence obligations will be expanded to any crime

---

<sup>48</sup> Australian Privacy Foundation, "Cybercrime Legislation Amendment Bill 2011, Submission to the Joint Standing Committee on Cyber-Safety," August 5, 2011.

<sup>49</sup> Law Council of Australia, "Submission No. 5, Inquiry into Cybercrime Legislation Amendment Bill 2011," Joint Select Committee on Cyber-Security, July 14, 2011, p. 3.

[http://www.aph.gov.au/Parliamentary\\_Business/Committees/House\\_of\\_Representatives\\_Committees?url=jssc/cybercrime\\_bill/subs.htm](http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=jssc/cybercrime_bill/subs.htm).

<sup>50</sup> Ibid.

<sup>51</sup> Section 5D of the *Telecommunications Act 1997*.

provided that a number of set procedural conditions are met. The data may be preserved but cannot be disclosed in the absence of a warrant.

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 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 with a valid warrant.<sup>52</sup>

There have been a number of politically-motivated cyberattacks, particularly distributed denial-of-service attacks (DDoS) that have led to websites being inaccessible or flooded with substituted content for various lengths of time. For example, offline marches and online acts of protest were staged in response to the Australian government's decision to introduce a mandatory filter in 2010. One of these protests was the online defacement and DDoS attack of the Australian Parliamentary website by the Anonymous hacktivist group, dubbed Operation Titstorm. The attack brought down the parliament's website for three days by bombarding it with pornographic images.<sup>53</sup> In 2011, Matthew George, an Australian member of Anonymous who participated in Operation Titstorm, was charged and convicted of incitement, and was given an AUS\$550 (US\$570) fine.<sup>54</sup> More severe cyberattacks on the nation's critical infrastructure (such as electric grids, hospitals, and banks) have occurred as well, though to date, attacks on banking institutions for financial motives have been much more frequent.<sup>55</sup>

---

<sup>52</sup> ACMA, "Pre-paid Mobile Services—Consumer Information Provision Fact Sheet," accessed June 2010, [http://www.acma.gov.au/WEB/STANDARD/pc=PC\\_9079](http://www.acma.gov.au/WEB/STANDARD/pc=PC_9079).

<sup>53</sup> Alana Maurushat, "Ethical Hacking (2012): A Report for A Report for the National Cyber Security Division of Public Safety Canada." Publication on file with author. Report to be released to the public in 2012.

<sup>54</sup> Sarah Whyte, "Meet the hacktivist who tried to take down the government," Sydney Morning Herald, March 14, 2011, <http://www.smh.com.au/technology/security/meet-the-hacktivist-who-tried-to-take-down-the-government-20110314-1brkt.html>.

<sup>55</sup> AusCERT Conference (2009), closed session invite-only workshop on cybercrime, Chatham House Rules.