



AUSTRALIA

	2012	2013
INTERNET FREEDOM STATUS	FREE	FREE
Obstacles to Access (0-25)	2	2
Limits on Content (0-35)	5	5
Violations of User Rights (0-40)	10	11
Total (0-100)	17+	18

POPULATION: 22 million
INTERNET PENETRATION 2012: 82 percent
SOCIAL MEDIA/ICT APPS BLOCKED: No
POLITICAL/SOCIAL CONTENT BLOCKED: No
BLOGGERS/ICT USERS ARRESTED: No
PRESS FREEDOM 2013 STATUS: Free

* 0=most free, 100=least free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Broadband access continued to expand for online users as the National Broadband Network reached more rural and remote communities (see **OBSTACLES TO ACCESS**).
- Concerns over ISP filtering practices continued, as it was revealed that a number of legitimate websites were accidentally blocked by ISPs who were trying to limit access to a fraudulent website with the same IP address (see **LIMITS ON CONTENT**).
- Australia’s accession to the Council of Europe’s Convention on Cybercrime in 2012 raised concerns about additional requirements in the Australian legislation for ISPs to monitor and store user data, especially in regard to the requirement to comply with foreign preservation notices (see **VIOLATIONS OF USER RIGHTS**).

INTRODUCTION

Australia enjoys affordable, high-quality access to the internet and other digital media, and this access has continued to expand over the past few years with the rollout of the National Broadband Network. However, 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 Although not currently law, there have been a number of proposals put forward on data retention, surveillance, and filtering in the course of the last two years.

Additionally, in late 2012 Australia acceded to the Council of Europe's Convention on Cybercrime, which brought into effect a number of obligations for ISPs to monitor, preserve, and store user data. However, the Australian legislation goes beyond the requirements set out in the Convention by requiring longer retention timelines for foreign preservation notices, and requiring ISPs to cooperate with any serious crime being investigated in Australia or overseas.

OBSTACLES TO ACCESS

In 1989, Australia's Academic and Research Network (AARNet) made the country's first internet connection with a 56 Kbps 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) in 2012,³ all Australians, including those in more remote areas, will soon have access to an internet connection with a peak speed of at least 12 Mbps for its mixed network (fiber, wireless and satellite technology), while the fiber product will offer speeds from 100 Mbps to 1 Gbps.⁴

Australia has an internet penetration rate of approximately 82 percent as of December 2012, according to the International Telecommunication Union.⁵ There were 12.2 million internet subscribers in Australia in December 2012 (excluding internet connections enabled through mobile phone handsets) and 17.4 million mobile handset subscribers.⁶ The internet penetration rate is

† The 2012 rating for Australia was adjusted on the basis of updated scoring guidelines to best convey changes over time.

¹ For a comprehensive overview of the legislative history of censorship in Australia see Libertus.net, "Australia's Internet Censorship System," accessed June 2010, <http://libertus.net/censor/netcensor.html>. See also Australian Privacy Foundation, accessed June 2010, <http://www.privacy.org.au>.

² Australia's Academic and Research 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/OzlHist.html>; Roger Clarke, "Origins and Nature of the Internet in Australia," January 29, 2004, <http://www.rogerclarke.com/II/Ozl04.html>.

³ 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.

⁴ NBN Co., "National Broadband Network," accessed January 10, 2013, <http://bit.ly/16U3Qvt>.

⁵ International Telecommunication Union, "Percentage of Individuals Using the Internet," accessed July 15, 2013, <http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>

⁶ Australian Bureau of Statistics, "Internet Activity, Australia," December 2012, <http://bit.ly/18eYL3l>.

expected to steadily increase with the implementation of the NBN, which includes expanded wireless and satellite services in rural communities. 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 phones.

Access to the internet and other digital media is widespread in Australia. Australians have a number of internet connection options, including ADSL, ADSL 2+, wireless, cable, satellite, and dial-up.⁷ Wireless systems can reach 99 percent of the population, while satellite capabilities are able to reach 100 percent. While the internet service provided by these systems can be slow, the expansion of the NBN means that all Australians will have access to high internet speeds. Major ISPs such as Telstra offer financial assistance for internet connections to low-income families.⁸ 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.⁹

Age is a significant indicator of internet use, with 69 percent of Australians between the ages of 18 and 24 accessing the internet at home on a daily basis and 75 percent of people 15 years or over reporting having used the internet over a 12 month period.¹⁰ By contrast, only 31 percent of those 65 years and over had used the internet in the same 12 months.¹¹

Approximately 50 percent of Aboriginal and Torres Strait Islanders living in discrete indigenous communities (i.e. not major cities) have access to the internet, with 36 percent having internet access in the home.¹² In remote indigenous communities, 63 percent of the population had taken up mobile phone services in 2004.¹³ However, not all indigenous communities have mobile phone coverage; the overall mobile phone penetration rate in Aboriginal communities is unknown.

Australia has a mobile phone penetration rate of 106 percent, with many consumers using more than one SIM card or mobile phone.¹⁴ Third generation (3G) mobile services are the driving force behind the recent growth, with 24.3 million mobile subscriptions operating in 2012.¹⁵

⁷ 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.

Australian Communications and Media Authority (ACMA), *Communications Report, 2010–11* (Canberra: ACMA, 2011), http://www.acma.gov.au/webwr/assets/main/lib410148/communications_report_2010-11.pdf.

⁸ Telstra, *Telstra Sustainability Report 2011*, accessed March 2013, <http://bit.ly/1dPRUQw>.

⁹ Australian Government National Broadband Network, “NBN Key Questions and Answers,” accessed June 2010. <http://www.nbn.gov.au/content/nbn-key-questions-and-answers-faqs>.

¹⁰ Australian Bureau of Statistics, “Online @ Home,” accessed March 2012, <http://bit.ly/mnrJiG>.

¹¹ Ibid.

¹² Australian Bureau of Statistics, “Internet Access at Home,” 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), accessed June 2010, http://www.acma.gov.au/WEB/STANDARD/pc=PC_311397.

¹³ Australian Communications and Media Authority (ACMA), *Communications Report, 2008–2009* (Canberra: ACMA, 2008–2009), http://www.acma.gov.au/webwr/assets/main/lib311252/08-09_comms_report.pdf. There is no equivalent data on indigenous communities in the more recent 2011–2012 report.

¹⁴ International Telecommunication Union, “Mobile-cellular telephone subscriptions,” accessed July 15, 2013, <http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>

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 affordability is not comparable to that in metropolitan areas.¹⁶

The government has adopted a strong policy of technological neutrality, also referred to as net 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 of traffic shaping. Some Australian ISPs and mobile service providers practice traffic shaping (also known as data 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

Like most other industrialized nations, Australia hosts a competitive market for internet access, with 81 medium-to-large ISPs as of June 2012, as well as a number of smaller ISPs.¹⁸ Many of the latter are “virtual” providers, maintaining only a retail presence and offering end users access through the network facilities of other companies; these providers are carriage service providers and do not require a license.¹⁹ 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 (TIO).²⁰ 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.²¹ The industry’s involvement consists of developing industry standards and codes of practice.²²

The ACMA is the primary regulator for the internet and mobile telephony, and is responsible for enforcing Australia’s anti-spam law.²³ Its oversight is generally viewed as fair and independent, though there are some transparency concerns with regard to the classification of content. Small businesses and residential customers may file complaints about internet, telephone, and mobile-phone services with the TIO,²⁴ which operates as a free and independent dispute-resolution service.

¹⁵ Australian Communications and Media Authority (ACMA), *Communications Report, 2011-2012* (Canberra: ACMA, 2011-2012), http://www.acma.gov.au/webwr/assets/main/lib550049/comms_report_2011-12.pdf. The Report was tabled to Parliament and released on Dec. 1, 2012.

¹⁶ Rural Broadband, “Welcome,” accessed June 2010, <http://www.ruralbroadband.com.au>.

¹⁷ Telstra, 19.

¹⁸ Australian Bureau of Statistics, “Internet Activity, Australia, June 2012,” <http://bit.ly/R9RsDo>.

¹⁹ Australian Bureau of Statistics, “Internet Activity, Australia, Dec. 2009,” <http://bit.ly/1fRWQpZ>.

²⁰ Australia Communications and Media Authority, “Carriage & Service Provider Requirements, accessed March 2013, http://www.acma.gov.au/WEB/STANDARD..PC/pc=PC_1622.

²¹ Australian Communications and Media Authority Act 2005, <http://bit.ly/16U44mm>;

Broadcasting Services Act 1992, http://www.austlii.edu.au/au/legis/cth/consol_act/bsa1992214/;

ACMA, “Service Provider Responsibilities,” accessed June 2010, http://www.acma.gov.au/WEB/STANDARD/1001/pc=PC_90157.

²² Chris Connelly and David Vaile, “Drowning in Codes: An Analysis of Codes of Conduct Applying to Online Activity in Australia,” Cyberspace Law and Policy Centre, March 2012, <http://cyberlawcentre.org/onlinecodes/report.pdf>.

²³ ACMA, “The ACMA Overview,” accessed March 2012, http://www.acma.gov.au/WEB/STANDARD/pc=ACMA_ORG_OVIEW;

ACMA, “About communications & media regulation,” accessed March 2012,

http://www.acma.gov.au/WEB/STANDARD/pc=PUB_REG_ABOUT.

²⁴ Telecommunications Industry Ombudsman, accessed March 2012, <http://www.tio.com.au>.

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. The ability to openly express dissatisfaction with politicians and to criticize government policies is not hindered by the authorities, and complaints may be sent directly to the Telecommunications Industry Ombudsman.²⁵ However, the legal guidelines and technical practices by which ISPs filter illegal material on websites have raised some concerns in the past year.

In 2010, the government proposed implementing a mandatory filtering system run through ISPs.²⁶ Draft legislation was proposed under the Rudd Labour government, and then put aside during the election in August 2010 when a minority government with Julia Gillard of the Labour Party came to power. While the Gillard government had stated that they might introduce legislation on this topic, there have been no formal proposals, bills, or further discussion on the matter since the election. Another election was planned for September 2013, but has been cancelled due to Kevin Rudd winning the Labour Party leadership vote, after which Gillard resigned and Rudd was sworn in as Prime Minister. So far, there have not been any claims by either party to introduce mandatory filtering. Despite the lack of mandatory filtering, ISPs still voluntarily block content from websites that are on Interpol's blacklist and that contain child pornography.

Controversy struck, however, in May 2013 when it was revealed that a number of legitimate Australian websites not hosting any type of illegal or even controversial material had been blocked. Investigations revealed that the Australian Security and Investment Commission was using an obscure provision (section 313) of the Telecommunications Act to request that a fraudulent website be blocked.²⁷ The notice by ASIC to the ISPs specified an IP address that contained the fraudulent website along with a number of legitimate websites, including that of Melbourne Free University. This is the first known incident of ASIC using s.313 to issue notices to ISPs to block non-Interpol material. The use of section 313 in this matter is highly contentious.

In addition, there are two systems in place that regulate internet content and place some restrictions on what can be viewed online. Under the first system, 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.²⁸ Under the Broadcasting Services Act, the following categories of online content are prohibited:

²⁵ Ibid.

²⁶ Alana Maurushat, Renee Watt, "Australia's Internet Filtering Proposal in the International Context," *Internet Law Bulletin* 12, no. 2 (2009); ACMA, "Service Provider Filtering", http://www.acma.gov.au/scripts/nc.dll?WEB/STANDARD/1001/pc=PC_90157

²⁷ LeMay, R., "Interpol Filter Scope Creep: ASIC Ordering Unilateral Website Blocks" (May, 15, 2013), accessed July 16, 2014, <http://delimitter.com.au/2013/05/15/interpol-filter-scope-creep-asic-ordering-unilateral-website-blocks/>

²⁸ Internet Society of Australia, "Who Is an Internet Content Host or an Internet Service Provider (and How Is the ABA Going to Notify Them?)" accessed June 2010, <http://www.isoc-au.org.au/Regulation/WhoisISP.html>;

- 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 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.²⁹

To date, there have not been any problems with this system of take-down notices being applied to videos, films, literature, or similar material with information of political or social consequence. In addition, the government's 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) if the regulator decides that the provider is not already doing so. Failure to comply with such instructions may draw a maximum penalty of AUD 11,000 (approximately USD 11,500) per day. Other regulatory measures require ISPs to offer their customers a family-friendly filtering service.³⁰ This practice is known as voluntary filtering, since customers must select it as an option.

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.³¹ The 1995 Classification Act and the 1992 Broadcasting Services Act were amended in 2012 to now include an R 18+ category for video games. The laws entered into force on January 1, 2013. In the past, the lack of an R 18+ classification for video games led to some peculiar results with games such as *Aliens vs. Predators* initially given an RC classification which

Internet Industry Association, "Guide for Internet Users," March 23, 2008, <http://bit.ly/1hfYKP7>.

²⁹ ACMA, "Prohibited Online Content," accessed June 2010, http://www.acma.gov.au/WEB/STANDARD/pc=PC_90102.

³⁰ 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.acma.gov.au/webwr/aba/contentreg/codes/internet/documents/content_services_code_2008.pdf

³¹ Libertus.net, "Australia's Internet Censorship System," <http://libertus.net/censor/netcensor.html>.

was later amended to M 15+.³² When a game is classified as RC, often the developer will slightly modify the game to ensure it receives either an R 18+ or an M 15+ ranking.³³

The classification system suffers from a lack of transparency; the ACMA does not inform Australian content owners when it issues a take-down notice, and there is no mechanism available for owners or creators to challenge the classification of RC content. Only the ISP or similar intermediary hosting the material may bring a challenge to the Administrative Appeals Tribunal (AAT). In February 2012, the Australian Law Reform Commission released their report on the introduction of a new classification scheme, with recommendations as to how the classification scheme should be amended and clarified.³⁴ However, none of the report's recommendations are currently being considered by Parliament, and legislation is not expected to be introduced in 2013.

There are no examples of online content manipulation by governments or partisan interest groups. 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.³⁵ Nevertheless, the need to avoid defamation and, to a lesser extent, contempt of court has been a driver of self-censorship by both the media and ordinary users (see "Violations of User Rights"). For example, narrowly-written suppression orders are often interpreted by the media in an overly broad fashion so as to avoid contempt of court charges.³⁶

Aside from the restrictions on prohibited content, the incitement of 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. In August and September of 2012, Australians vocalized their opinions about the Attorney-General's proposal regarding data retention and the introduction of surveillance mechanisms that would store users' online and mobile phone communications for two years. The proposal was immensely unpopular with the industry, civil liberties groups, and general consumers. Groups such as *Getup!* encouraged Australians to send e-mails and twitter messages to Nicola Roxon, the Attorney-General, to voice their concerns over the proposal. As a result of the immense unpopularity of the data retention proposal, Roxon released a video on YouTube in which she attempted to clarify some of the key aspects of the proposal that had been criticized.³⁷

³² Australian Government – Classification Review Board 2009, *Alien vs. Predator – Review Board Decision Reasons*, accessed March 2013, <http://www.classification.gov.au/About/Documents/Review%20Board%20decisions/DecisionReasons-AliensvsPredator-Final-4January2010.pdf>.

³³ See generally Andy Chalk, "OFLC reveals changes to Australian *Fallout 3*," *The Escapist*, 13 August 2000, <http://www.escapistmagazine.com/news/view/85646-OFLC-Reveals-Changes-To-Australian-Fallout-3>.

³⁴ Australian Law Reform Commission Report 118, "Classification-Content Regulation and Convergent Media" February 2012, http://www.alrc.gov.au/sites/default/files/pdfs/publications/final_report_118_for_web.pdf.

³⁵ *Jones v. Toben* [2002] FCA 1150 (17 September 2002), <http://www.austlii.edu.au/au/cases/cth/FCA/2002/1150.html>.

³⁶ Nick Title, "Open Justice – Contempt of Court" (paper presentation, Media Law Conference Proceedings, Faculty of Law, The University of Melbourne, February 2013).

³⁷ Delimiter, "Roxon Makes Plea on YouTube," September 11, 2012, <http://delimiter.com.au/2012/09/11/data-retention-roxon-makes-youtube-plea/>.

Advanced web applications like 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. 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.³⁸

VIOLATIONS OF USER RIGHTS

While online 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. Australia's accession to the Council of Europe Convention on Cybercrime on November 30, 2012, while putting the country in line with international legal standards, also raised concerns because of the broader requirements under the Australian legislation for ISPs to monitor user activities.

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.³⁹ 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, further protected by an independent judiciary. The country is also a signatory to the International Covenant on Civil and Political Rights (ICCPR).

The Australian press, however, has consistently expressed concerns about a "culture of secrecy" that continues to inhibit reporting.⁴⁰ 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 350 pieces of legislation containing "secrecy" provisions to restrict media publications.⁴¹ There are two significant secrecy laws that have a far-reaching impact on the media. The first is a lack of federal legislation to protect whistleblowers. The second is a lack of shield laws in many Australian states, which means that journalists are not shielded from having to disclose their sources in a court proceeding. In cases where journalists do not disclose their sources, they are subject to

³⁸ 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) *Media International Australia Incorporating Culture and Policy*, pp. 5-13. Also available at <http://eprints.qut.edu.au/39366/1/c39366.pdf>

³⁹ Alana Maurushat, Renee Watt, "Australia's Internet Filtering Proposal in the International Context," *Internet Law Bulletin* 12, no. 2 (2009).

⁴⁰ David Rolph, Matt Vitins, and Judith Bannister, *Media Law: Cases, Materials and Commentaries* (South Melbourne: Oxford University Press, 2010): 44.

⁴¹ Australia's Right to Know, "Submission to the Australian Law Reforms Commission's Review of Secrecy Laws" (2007) <http://www.australiasrighttoknow.com.au/files/docs/ALRC-Secrecy-Submission.pdf>.

liability and possible criminal sanction.⁴² In October 2012, Independent Member of Parliament Andrew Wilke introduced the Public Interest Disclosure (Whistleblower Protection) Bill. The bill is consistent with past recommendations and committee outcomes recommending that whistleblower protection be introduced at the federal level. The bill, if enacted, provides much needed protection for those federal public sector employees who leak information about corrupt practices. At this time there is no evidence to support whether leaking information occurs more often via online communication as opposed to traditional media such as print or broadcast.

The Anti-Terrorism Act 2005 (Cth) revived laws against sedition and unlawful association. The unlawful association provisions have been used widely since their enactment to ban several organizations perceived to be potentially dangerous in terms of their links to violent acts.⁴³ The sedition provisions, however, have not been used. Further, insults against government institutions or officials would not fall within the sedition provisions.⁴⁴

Australian defamation law has been interpreted liberally and is governed by legislation passed by the states as well as common law principles.⁴⁵ Civil actions over defamation are common and form the main impetus for self-censorship,⁴⁶ though a number of cases have established a constitutional defense when the publication of defamatory material involves political discussion.⁴⁷ Court costs and stress associated with defending against suits under Australia's expansive defamation laws have caused organizations to leave the country and blogs to shut down.⁴⁸

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, in which individuals may take up legal cases in Australia because of the more favorable legal environment regarding defamation suits. The right to reputation is generally afforded greater protection in countries like Australia and the United Kingdom than the right of freedom of expression. In Australia this is especially so as freedom of expression is limited to political speech. While the United States and the United Kingdom have recently enacted laws to restrict libel tourism, Australia is not currently considering any such legislation.

Social-networking companies such as Twitter and Facebook are finding themselves in Australian courts under Australia's defamation laws. Recently, television actress and producer Marieke Hardy

⁴² 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/fofreport5.pdf>. See also LexMedia Australia, "Journalist Shield Laws in Australia" (2010) <http://www.lexmedia.com.au/2010/10/journalist-shield-laws.html#.UTfUOHnh2F8>.

⁴³ Andrew Lynch and George Williams, *What Price Security?* (UNSW Press: Sydney, 2006), 41-59.

⁴⁴ *Ibid.*

⁴⁵ Principles of online defamation stem from the High Court of Australia, *Dow Jones & Company Inc v. Joseph Gutnick*, [2002] HCA 56.

⁴⁶ Moss, 42.

⁴⁷ Human Rights Constitutional Rights, "Australian Defamation Law," <http://www.hrcr.org/safrica/expression/defamation.html>, accessed June 2010.

⁴⁸ Asher Moses, "Online Forum Trolls Cost me Millions: Filmmaker," *Sydney Morning Herald*, July 15, 2009, <http://www.smh.com.au/technology/technology-news/online-forum-trolls-cost-me-millions-filmmaker-20090715-dl4t.html>.

wrongly named Melbourne resident Joshua Meggitt as the author of a hate blog.⁴⁹ Hardy tweeted the defamatory comment, which was then retweeted by some of Hardy's followers. In 2011, Meggitt sued Hardy for defamation and reached a confidential settlement out of court. Then in 2012, Meggitt took further legal action against Twitter as the publisher of Hardy's defamatory tweet. Hardy has reached a confidential settlement out of court. There is no reported outcome yet in the Twitter matter.

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 providing there is a valid warrant.⁵⁰

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).⁵¹ 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.⁵² Unlawful collection and disclosure of the content of a communication can draw both civil and criminal sanctions.⁵³ 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.⁵⁴

On August 22, 2012, the Australian Senate passed the Cybercrime Legislation Amendment Bill, allowing Australia to accede to the Council of Europe Convention on Cybercrime.⁵⁵ Unlike that of many other countries that have already ratified the convention, Australia's legislation goes beyond the treaty's terms by 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 restricted to the areas in the Convention: child pornography, online copyright (intellectual property), online

⁴⁹ Michelle Griffin, "Man Sues Twitter over Hate Blog" *Sydney Morning Herald*, February 17, 2012, <http://www.smh.com.au/technology/technology-news/man-sues-twitter-over-hate-blog-20120216-1tbwg.html>.

⁵⁰ ACMA, "Pre-paid Mobile Services—Consumer Information Provision Fact Sheet," accessed June 2010, http://www.acma.gov.au/WEB/STANDARD/pc=PC_9079.

⁵¹ Telecommunications Act 1997, Part 13, http://www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/.

⁵² Part 2-1, section 7, of the Telecommunications (Interception and Access) Act 1979 (TIAA) prohibits disclosure of an interception or communications, and Part 3-1, section 108, of the TIAA prohibits access to stored communications. See Telecommunications (Interception and Access) Act 1979, http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/.

⁵³ Criminal offenses are outlined in Part 2-9 of the TIAA, while civil remedies are outlined in Part 2-10. See Telecommunications (Interception and Access) Act 1979, http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/.

⁵⁴ Alana Maurushat, "Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Obfuscation Crime Tools?" (2010) *University of New South Wales Law Journal* 16, no. 1.

⁵⁵ Council of Europe, Convention on Cybercrime, <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG>.

fraud and forgery, and computer offenses. The new Australian legislation compels ISP cooperation for any serious crime being investigated in Australia or overseas; it is not limited to the crimes set out in the Convention.

The Convention also requires expeditious preservation of data by the person in possession or control of data, which means ISPs will often be the ones called upon to preserve data. Articles 16 and 17 of the Convention state that ISPs can be compelled to preserve internet traffic data logs for a maximum period of 90 days, whereas the Australian legislation mandates that ISPs store data for 180 days for foreign preservation notices. However, the Convention does not compel ISPs to monitor stored communications, only traffic data. In the case of an active criminal investigation, the Convention obligates an ISP to preserve the data that is already stored but would otherwise be deleted. This could include preservation of what IP addresses connect to and from other IP addresses, or what phone numbers connect to a Voice over Internet Protocol (VoIP) number. This may also include information about what types of protocols a customer uses, the size and use of packets, and so forth. Data preservation remains a controversial point but most notably in relation to the obligation to provide mutual assistance to a foreign entity.

In July 2012, the Commonwealth Attorney-General's Department released a discussion paper titled "Equipping Australia against emerging and evolving threats."⁵⁶ Under the proposal, Australian ISPs would be required to monitor, collect, and store information pertaining to all users' communications, including storing communications for a period of two years. This activity would be done without a warrant and enforced against all users regardless of whether there is a criminal investigation.⁵⁷ A similar data retention law is in place in Europe.⁵⁸ Many European courts, however, have struck down the data retention provisions on the grounds that they are a gross violation of privacy, inconsistent with domestic law, and unconstitutional.⁵⁹ The Attorney-General has failed to discuss the significant differences between the EU and Australian legal environments. In EU countries, including the United Kingdom, citizens' human rights are protected under a Bill of Rights or a Charter of Human Rights and Freedoms. Like the U.S. courts, European courts can strike down laws or directives which offend these guarantees of fundamental human rights and civil liberties. There is no Bill of Rights or Charter of Human Rights and Freedoms in Australia. As such, the courts have no effective means to strike down proposals that violate civil liberties. Once a proposal is enacted, the only way to have it changed is through legislation, which often requires a change of government. This compulsory data-retention policy, if enacted, could become a significant threat to online freedom in Australia. The proposal is not yet official policy in Australia, nor has it evolved to a bill. At this point in time it remains a proposal only.

⁵⁶ Commonwealth Attorney-General's Department's Discussion Paper, *Equipping Australia against emerging and evolving threats*, 2012, accessed February 1, 2013, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjicis/nsl2012/additional/discussion%20paper.pdf.

⁵⁷ 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>.

⁵⁸ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006

⁵⁹ Countries that have annulled, modified, or ruled the provisions unconstitutional include: Germany, Czech Republic, Romania, Bulgaria, and the Republic of Cyprus. Constitutional challenges continue in Ireland, Hungary, and Slovakia.

There have been several cases in the states of New South Wales and Victoria of individuals being sentenced to jail terms for publishing explicit photos of women, typically former girlfriends or boyfriends. By way of example, Australian citizen Ravshan Usmanov pled guilty to publishing an indecent article and was originally sentenced to six months of home detention after he posted nude photographs of an ex-girlfriend on Facebook.⁶⁰ The sentence was appealed and the court commuted the original sentence in favor of a suspended sentence.

The group Anonymous has commenced a series of “hacktivist” attacks in response to the data retention proposal put forth by the Attorney-General. In July 2012, the movement took down a number of government websites as a form of protest after a Q&A session with Julia Gillard in which details of many cybersecurity initiatives were outlined.

⁶⁰ Heath Astor, “Ex-Lover Punished for Facebook Revenge,” April 22, 2012, *Sydney Morning Herald*, <http://www.smh.com.au/technology/technology-news/exlover-punished-for-facebook-revenge-20120421-1xdpy.html>.