Australia and New Zealand Overview

Australia maintains some of the most restrictive Internet policies of any Western country and over the past two years has taken steps toward a nationwide mandatory Internet filtering scheme. Its neighbor, New Zealand, regulates the Internet considerably less rigorously. Australia's constitution does not explicitly give the right to free speech,[1] and in fact contains a clause giving the Australian government "communications power," allowing it to regulate "postal, telegraphic, telephonic, and other like services," including the Internet.[2] A number of state and territorial governments in Australia have passed legislation making the distribution of offensive material a criminal offense, as the constitution does not afford that power to the national government.[3]

The Australian government has for some time promoted and financed an "opt-in" filtering program, in which users voluntarily accept filtering software that blocks offensive content hosted outside the country. In 2008, the government announced plans for a layered filtering scheme, proposing a mandatory filter to block pornographic and illegal content, as well as an opt-out filter that would block even more content. The filter, which faces considerable opposition from Australian and international anti-censorship groups and, in some cases, the ISPs themselves, will first be tested by six ISPs before going live.[4]

In contrast, New Zealand has less strict Internet regulations. The government maintains a more limited definition of offensive content that can be investigated by a designated government entity, although—unlike in Australia—the definition includes hate speech (despite its being illegal in both countries). Furthermore, the government of New Zealand has not passed legislation to allow issuance of takedown notices for such content, and its enforcement of Internet content regulation by prosecution almost solely focuses on child pornography. New Zealand has not yet formalized its copyright laws and has rejected multiple proposals to do so, most recently scrapping proposed Section 92A of the Copyright Amendment (New Technologies) Act.[5] The country's defamation and surveillance laws are similar to those of Australia. Overall, Australian Internet regulations are significantly stricter than those of New Zealand and much of the Western world.

Offensive Content

Australia's and New Zealand's approaches to offensive content on the Internet both rely on government-run content-classification systems. However, their approaches differ in terms of what is considered offensive and what is done about the offending content.

Australian laws relating to the censorship of offensive content are based on the powers delineated in and protections omitted from the Australian constitution. Section 51(v) of the document gives Parliament power to "make laws for the peace, order, and good government of the Commonwealth with respect to: (v) postal, telegraphic, telephonic, and other like services."[6] With no explicit protection of free speech in the constitution, the Australian government has invoked its "communications power" to institute a restrictive regime of Internet content regulation.

The Broadcasting Services Amendment (Online Services) Bill 1999, an amendment to the Broadcasting Services Act 1992, establishes the authority of the Australian Communications and Media Authority (ACMA)[7] to regulate Internet content. The ACMA is empowered to look into complaints from Australians about offensive content on the Internet and issue takedown notices. The ACMA is not mandated to scour the Internet for potentially prohibited content, but it is allowed to begin investigations without an outside complaint.[8]

Web content that is hosted in Australia may be subject to a takedown request from the ACMA if the Office of Film and Literature Classification finds that it falls within certain categories as defined by the Commonwealth Classification (Publications, Films and Computer Games) Act 1995, a cooperative classification system agreed to by the national, state, and territorial governments.

The levels and definitions of prohibited content are as follows:

1. R18: Contains material that is likely to be disturbing to those under 18. This content is not prohibited on domestic hosting sites if there is an age-verification system certified by the ACMA in place.
2. X18: Contains nonviolent sexually explicit content between consenting adults. This content may be subject to ACMA takedown provisions if hosted on domestic servers.
3. RC: Contains content that is Refused Classification (child pornography, fetish, detailed instruction on crime, etc.) and is prohibited on Australian-hosted Web sites.[9]

The classification system chosen for Internet content is the more restrictive standard used for films, rather than the publications classification. As a result, some content allowable offline is banned when brought online.[10]

Once the determination has been made that content hosted within Australia is prohibited, the ACMA issues a takedown notice to the Internet content provider (ICP). It is not illegal for the ICP to host prohibited content, but legal action could be taken against it by the government if it does not comply with the takedown notice.

For offensive content hosted outside of Australia, the ACMA itself determines whether content is prohibited and notifies a list of certified Web-filter manufacturers to include the prohibited Web sites in their filters.[11] To obtain certification, these certified ''Family Friendly Filters'' must agree to keep lists of prohibited sites confidential.[12] Providers are then required to offer a Family Friendly Filter to all their customers, though customers are not required to accept them.[13] As a result, content taken down in Australia could be posted outside the country and still be accessible to the majority of Australian Internet users. Electronic Frontiers Australia, a nonprofit group dedicated to protecting online freedoms, reports that at least one Web site taken down has moved to the United States, even keeping its URL under the ''.au'' domain. It is not known how many Web sites have moved overseas in this fashion.[14]

States and territories in Australia have instituted a variety of laws that criminalize the downloading of illegal content and the distribution of content that is ''objectionable'' or ''unsuitable for minors.''[15] The state of Victoria, for example, in Section 57 of its Classification (Publication, Films and Computer Games) (Enforcement) Act 1995, makes it illegal to ''use an on-line information service to publish or transmit, or make available for transmission, objectionable material.''[16] There is no uniformity between the states, however. In Western Australia, for example, it is not illegal to distribute R18 and X18 to adults online (though the ACMA can still issue takedown notices), but the possession of any RC content (not just child pornography, as is the case in other states) is illegal.[17]

In March 2007, all mainland states in Australia banned access to YouTube over school networks because of an uploaded video depicting a 17-year-old Australian girl

being abused, beaten, and humiliated by a group of young people. Eight youths have been charged in connection with the assault.[18] School blocking of YouTube has faced opposition, notably from Google executive Vint Cerf, who noted his belief that ''many young people have those skills that may be well beyond those of their parents and their teachers and will find ways of accessing information.''[19]

The Commonwealth is also implementing new Internet filtering initiatives. In June 2006, the Australian government announced an AUD 116.6 million initiative, ''Protecting Australian Families Online.'' The initiative included AUD 93.3 million to be spent over three years to provide all families with free Web filters. The government also announced that it would test an ISP-level blocking system in Tasmania. At the time, Helen Coonan, the minister for communications, information technology, and the arts, opposed implementing this system on a countrywide basis.[20]

However, in December 2007, Telecommunications Minister Stephen Conroy announced a strengthened ''clean feed'' policy, under which all Australian ISPs are required to provide Internet filtering services that prevent child pornography and other ''inappropriate'' material from reaching schools and houses.[21] Those who link to banned sites from their own sites will be fined AUD 11,000 per day.[22] Instead of opting in to the program, as users did under the 2006 initiative, users who wish to see adult material must opt out (there is no opt-out for illegal content). In conjunction with the new policy, the ACMA released a set of updated regulations entitled the Restricted Access System Declaration of 2007,[23] requiring content service providers to implement age-verification systems on all Web sites containing mature or adult content.[24] As of April 2009, ACMA was still conducting trials for ISP-level content filtering; eight ISPs had agreed to participate.[25]

The plan was initially kept under wraps. In October 2008, a policy advisor in Conroy's office sent an e-mail to the Internet Industry Association (IIA) instructing the IIA to inform ISPs that they must keep quiet about the country's filtering scheme.[26] The incident was widely reported by the Australian press, and several heads of ISPs spoke out against what they considered to be an attempt at censorship.[27]

One concern of those opposed to the scheme is the potential for nonillegal Web sites to be banned, a fear that has turned out not to be unfounded. In March 2009, ACMA added pages from the whistle-blowing site Wikileaks to its blacklist of banned URLs after the site published a secret Internet censorship list for Denmark.[28] In doing so, Australia became one of only three countries in the world to censor the site—the other two are China and the United Arab Emirates. In retaliation, a group of anonymous activists published ACMA's confidential blacklist on Wikileaks.[29]

Although New Zealand has not yet instituted a filtering scheme like that which Australia is working to implement, a vaguely worded page on the Department of Internal Affairs' (DIA) special censorship page entitled ''Censorship and the Internet'' states that the department ''takes a proactive role in prosecuting New Zealanders who trade

objectionable material via the Internet. If a publication is categorised as 'objectionable' it is automatically banned by the Films, Videos, and Publications Classification Act 1993.''[30] Electronic Frontiers Australia has stated that this act likely covers Internet materials as well.[31] Under the act, any material that ''describes, depicts, expresses, or otherwise deals with matters such as sex, horror, crime, cruelty, or violence in such a manner that the availability of the publication is likely to be injurious to the public good'' is considered objectionable and is illegal to distribute or possess.[32] Specifically, any material that promotes or supports ''the exploitation of children, or young persons, or both, for sexual purposes; or the use of violence or coercion to compel any person to participate in, or submit to, sexual conduct; or sexual conduct with or upon the body of a dead person; or the use of urine or excrement in association with degrading or dehumanizing conduct or sexual conduct; or Bestiality; or acts of torture or the infliction of extreme violence or extreme cruelty'' is banned.[33] There is also a decision procedure described in the act for any content that might be objectionable but does not fall within this specific list, including discriminatory and hateful material.[34] This law has formed the basis of the DIA's enforcement of Internet censorship in the country.

Like Australia's ACMA, the DIA ''proactively'' investigates potentially banned material[35] and submits any such material not already classified to the Office of Film and Literature Classification for a ruling.[36] This office then classifies the material as ''unrestricted'' or ''objectionable,'' except in certain circumstances of restricted access or for ''educational, professional, scientific, literary, artistic, or technical purposes.''[37]

There is, however, no explicit legal mechanism for the takedown of objectionable material. Instead, the nonprofit InternetNZ is in the process of establishing an industry-wide code of conduct that would require its signatories to agree not to host illegal content.[38] As a result, the government focuses its efforts on prosecuting the distributors or possessors. The Films, Videos, and Publications Classifications Amendment Act 2005 sets the penalty for distributing objectionable material at a maximum of ten years in prison (up from a maximum of one year) and for knowingly possessing objectionable materials at a maximum of five years in prison or a NZD 50,000 fine.[39] According to various sources, the DIA has almost completely focused its enforcement of Internet censorship on child pornography.[40]

Hate Speech

Both Australia and New Zealand have legislation addressing hate speech generally, and both have applied this legislation to the Internet through different means. New Zealand, however, has an institutionalized investigation system, while Australia does not.

Australia addresses hate speech through the Racial Discrimination Act 1975, which makes it ''unlawful for a person to do an act, otherwise than in private, if: the act is reasonably likely, in all the circumstances, to offend, insult, humiliate or intimidate

another person or a group of people; and the act is done because of the race, colour or national or ethnic origin of the other person, or of some or all of the people in the group.''[41]

Australian courts applied this law to the Internet for the first time in October 2002 in the *Jones v. Töben* case. Jeremy Jones and the Executive Council of Australian Jewry brought a lawsuit against Frederick Töben, the director of the Adelaide Institute, because of material on Töben's Web site (www.adelaideinstitute.org) that denied the Holocaust. The Federal Court, ruling that publication on the Internet without password protection is a ''public act,'' found that posting this material online was in direct violation of Section 18C of the Racial Discrimination Act 1975 (quoted earlier) and called for the material to be removed from the Internet.[42]

Australia does not, however, give the ACMA authority to investigate complaints or issue takedown notices for hateful or racist materials online, even if they would be illegal under the Racial Discrimination Act 1975.[43] Schedule 5 of the Broadcast Services Act 1992 gives the ACMA authority only over materials deemed ''offensive'' within the classification scheme described earlier. As a result, there appears to be no venue other than the courts in which to pursue complaints about hateful or racist materials online. However, Chilling Effects reports that Google received notice on May 5, 2006, of a site in its search results that ''allegedly violates section 18C of the Racial Discrimination Act 1975'' and removed it from the Google Australia site (www.google.com.au).[44] This action may be indicative of a new notice-based system taking form.

New Zealand, in contrast, has both explicit prohibition of discrimination based on race, religion, age, disability, and sexual orientation in Section 21(1) of the Human Rights Act 1993[45] and explicit prohibition of the publication of material that ''represents (whether directly or by implication) that members of any particular class of the public are inherently inferior to other members of the public by reason of any characteristic of members of that class, being a characteristic that is a prohibited ground of discrimination specified in Section 21(1) of the Human Rights Act 1993''[46] in Section 3e of the Films, Videos, and Publication Classifications Act 1993. The DIA uses these statutes to pursue investigations into potentially discriminatory material.

Copyright

Australia's copyright laws underwent a significant overhaul following the acceptance of the Australia–United States Free Trade Agreement in 2004. Pursuant to that agreement, Australia was required to bring its copyright laws closer in line with those of the United States.[47] Some of the relevant requirements included the following:

1. Agreeing to World Intellectual Property Organization (WIPO) Internet treaties.
2. Implementing an ''expeditious'' takedown system of copyright-infringing materials.

3. Strengthening control over copyright protection technology circumvention.
4. Agreeing to copyright protection standards.
5. Increasing the length of copyright to life plus seventy years from its previous level of life plus fifty years.[48]

Most of these provisions were implemented in the U.S. Free Trade Agreement Implementation Act 2004, though new regulations in response to requirement 3 were recently implemented in the Copyrights Amendment Act 2006.[49]

After implementing a system of copyright more consistent with that of the United States, the Australian government decided to pursue another overhaul of its copyright laws in 2006, as *ABC Science Online* reports, to "keep up with the rapidly changing digital landscape."[50] The proposed amendments to the Copyright Act 1968 were worrisome to many. Google argued that certain provisions would allow copyright owners to pursue legal action against it and other search engines for caching material without obtaining express permission from each Web site. These provisions would "condemn the Australian public to the pre-Internet era," Google argued.[51] Other critics contended that the proposed amendments would make possession of an iPod or other music-listening device designed to play MP3 files illegal, and uploading a video of oneself singing along to a pop song a crime.[52]

Although these two final concerns have been remedied in the resulting Copyrights Amendment Act 2006 (it is still legal to own an iPod and it is allowable to post a lip-synching video),[53] the caching issue still appears to be unresolved. There is an exception in the act that allows computer networks of educational institutions to cache copyright-protected online material "to facilitate efficient later access to the works and other subject-matter by users of the system."[54] However, this provision does not appear to offer the exception that Google sought.

Overall, though, the amendments allow for a greater number of exceptions to the copyright laws to establish more realistic fair use of copyrighted material, such as "time-shifting, format-shifting and space-shifting" (recording a television show to watch later, scanning a book to view it electronically, and transferring material from CDs to iPods, respectively), and greater protection of parody and satire.[55]

The Australian judiciary has been active in copyright enforcement online as well. In a landmark decision in December 2006, the Federal Court upheld a lower court ruling that found the Web site operator of mp3s4free.net, Stephen Cooper, and the hosting ISP, E-Talk, liable for copyright infringement. Cooper's site did not itself host any copyright-protected material, but rather served as a search engine through which users could find and download copyright-protected music for free. In its ruling, the court found that merely linking to copyright-protected material was grounds for infringement. In addition, the court found that ISP E-Talk was also liable for copyright infringement because it posted advertisements on the site and was unwilling to take the

site down.[56] Interestingly, Dale Clapperton, of Electronic Frontiers Australia, has argued that this decision could be used against search engines such as Google. In an article in the *Sydney Morning Herald*, he stated that "what Cooper was doing is basically the exact same thing that Google does, except Google acts as a search engine for every type of file, while this site only acts as a search engine for MP3 files."[57]

In New Zealand, recent attempts to regulate copyright law to include digital provisions have been rejected by the national government.[58] Therefore, New Zealand's current law is contained within the Copyright Act 1994. The term of a copyright is set at life plus fifty years.[59]

The Copyright (New Technologies and Performers' Rights) Amendment Bill currently being considered in New Zealand, however, would dramatically change the digital copyright landscape into one that more closely mirrors the Digital Millennium Copyright Act (DMCA) of the United States. If passed, the bill would allow for format shifting and space shifting of music,[60] criminalize the distribution of the means to subvert technological protection measures protecting copyrighted content, and establish a system in which ISPs are required to remove copyright-infringing content and notify the poster if the ISP "obtains knowledge or becomes aware that the material is infringing."[61] This removal system is somewhat different from the U.S. system of notice and takedown in that it requires knowledge of infringement and not simply notification.[62]

Defamation

Through a variety of court cases, both Australia and New Zealand have applied their respective defamation laws to the Internet, and both countries, with New Zealand courts following the Australian courts' example, have controversially expanded their jurisdiction in defamation suits to online materials hosted outside their borders.

Defamation in Australia, except for a small range of cases, is handled through state and territorial law;[63] until December 2005, states and territories maintained largely nonuniform codes of defamation.[64] After what amounted to a threat that the Commonwealth would act if states and territories did not, the states and territories finally decided to enact uniform laws in December 2005.[65] Since defamation laws are applied where material is seen, read, or experienced, nonuniform laws meant that writers and publishers had to be wary of different sets of laws all over the country under which they might be sued under various definitions of defamation.[66] Now the laws are uniform, so this liability risk has been mitigated. No legislation specifically targets defamation on the Internet, and, therefore, its regulation is essentially the same as that for all other publications.[67]

The judiciary has played an important role in setting online defamation policy because of jurisdictional issues. In a major decision in December 2002, the Australian

High Court ruled that a party within Australia can sue a foreign party in Australian court for defamation resulting from an online article hosted on a foreign server. The specific case involved a lawsuit pitting Joseph Gutnick, an Australian businessman, against Dow Jones over a defamatory article written about him in Barron's Online in October 2000. Dow Jones argued that since its servers (and therefore the article) were in the United States, the defamation case should have been tried in the United States. A decision allowing the case to be tried in Australia, they argued, would restrict free speech around the world because it would require authors and publishers to take into account the laws of foreign countries under which they could be sued when publishing material online.[68]

The court countered, however, that the ''spectre of 'global liability' should not be exaggerated. Apart from anything else, the costs and practicalities of bringing proceedings against a foreign publisher will usually be a sufficient impediment to discourage even the most intrepid of litigants. Further, in many cases of this kind, where the publisher is said to have no presence or assets in the jurisdiction, it may choose simply to ignore the proceedings. It may save its contest to the courts of its own jurisdiction until an attempt is later made to enforce there the judgment obtained in the foreign trial. It may do this especially if that judgment was secured by the application of laws, the enforcement of which would be regarded as unconstitutional or otherwise offensive to a different legal culture.''[69] The parties eventually settled for AUD 180,000 in damages and AUD 400,000 in legal fees.''[70]

New Zealand defamation law was first found to apply to online material in a district court decision, *O'Brien v. Brown*, in late 2001. In the case, Patrick O'Brien, chief executive officer of the New Zealand domain manager Domainz, sued Alan Brown, the head of a Manawatu ISP, for Brown's posting of harsh criticisms and calls for fraud investigation into Domainz on a publicly available Internet Society of New Zealand bulletin board.[71] The judge in the case found that the Internet afforded no additional freedom of expression to the defendant than any other medium and, further, that publication on the Internet required a greater award of damages than through another medium because of the ease with which Domainz's potential customers and clients could access the defamatory material.[72]

In addition, the New Zealand courts have followed Australia's example in determining the jurisdiction for defamation suits over online content hosted in a foreign country. Ironically, the relevant suit involved an Australian defendant. In 2004, the Wellington High Court found that the University of Newlands (based in New Zealand) could sue Nationwide News, Ltd. (based in Australia) in New Zealand court for Nationwide's inclusion of the plaintiff in a list of ''Wannabe Unis'' and ''degree mills'' in its online newspaper, *The Australian*. This ruling more closely aligned New Zealand defamation policy with Australia.[73]

Surveillance

Both Australia and New Zealand have taken steps toward greater Internet security, passing laws to give government agencies greater authority to investigate illegal activities online.

Australia's Internet surveillance regime is primarily based on two laws. The first is the Telecommunications (Interception and Access) Act 1979. This act, amended in June 2006, prohibits intercepting telecommunications or accessing, without first notifying both the sender and the receiver, stored telecommunications by any person or entity, except in cases such as the installation or maintenance of telecommunications equipment.[74] It also establishes two warrant systems, controlled by the attorney general, by which law enforcement may gain access to these communications: ''telecommunications service warrants'' (for real-time interception) and ''stored communications warrants'' (for access to stored communications without a requirement to notify the communicants).[75]

The second relevant law is the Surveillance Devices Act 2004, which significantly increases the authority of law enforcement to install surveillance devices such as keystroke recorders under newly created ''surveillance device warrants.''[76] Electronic Frontiers Australia has expressed worry that these warrants will be used by law enforcement to avoid applying for a telecommunications service warrant, essentially allowing them to intercept communications where a telecommunications service warrant would not have been authorized.[77]

Further, in 2003, the Australian Internet Industry Association (IIA) attempted to establish a code of practice requiring ISP signatories to retain user information for six or twelve months and provide it to law enforcement upon official request. Specifically, personal data—such as name, address, and credit card details—were to be retained by ISPs for six months after a customer ends service with that ISP or twelve months after the record is created, whichever is longer. Operational data, such as proxy logs and e-mail information, were to be kept for six months after creation of the data.[78] Law enforcement could request this information using the certificate system set up in the Telecommunications Act 1997,[79] which allows private information to be disclosed if ''an authorized officer of a criminal law-enforcement agency has certified that the disclosure is reasonably necessary for the enforcement of the criminal law.''[80]

In New Zealand, the most relevant piece of legislation to Internet security is Supplemental Order Paper 85 to the Crimes Amendment Bill No. 6, passed in 2003. The act essentially makes it illegal to hack or intercept electronic communications, but exempts the police, the Security Intelligence Service, and the Government Communications Security Bureau acting under interception warrants as described by the Crimes Act 1961. As noted on the Web site of the Green Party, however, these warrants could be ''quite broad in their application and cover a class of people.''[81]

Conclusion

Australian laws and policies toward the Internet are aligned with those of many Western countries, while New Zealand's are less stringent. The Australian government has instituted a strict takedown regime for offensive content, and various states and territories have made distribution of such content a criminal offense. The government is pursuing voluntary programs to increase home filtration of the Internet, and Australia's evolving hate speech, copyright, defamation, and security policies offer further justification for restricting Internet content. A countrywide ISP-level filtering scheme is currently being tested.

New Zealand, in contrast, has instituted a more limited classification system—though it does include hate speech—with no takedown notices and has not yet formally adopted copyright legislation that applies to the Internet. Its broad defamation and security policies, however, are more reminiscent of Australia.

Overall, however, Australia's Internet censorship regime is strikingly severe relative to both its neighbor and similar Western states, and it is helping to push the normative boundaries of filtering for an industrialized democratic state. It is not, however, at the level of the most repressive regimes that the OpenNet Initiative has studied.

Notes

1. Roy Jordan, "Free Speech and the Constitution," Parliamentary Library, June 4, 2002, http://www.aph.gov.au/LIBRARY/Pubs/RN/2001-02/02rn42.htm.

2. Geraldine Chin, "Technological Change and the Australian Constitution," *Melbourne University Law Review*, 25 (2000), http://www.austlii.edu.au/au/journals/MULR/2000/25.html.

3. Electronic Frontiers Australia, "Internet Censorship Laws in Australia," March 31, 2006, http://www.efa.org.au/Issues/Censor/cens1.html.

4. Fran Foo, "Green Light for ISP Filtering Trials," *Australian IT*, February 11, 2009, http://www.australianit.news.com.au/story/0,24897,25040645-15306,00.html.

5. Chris Keall, "Section 92A to Be Scrapped," *National Business Review*, March 23, 2009, http://www.nbr.co.nz/article/section-92a-be-scrapped-89121.

6. Geraldine Chin, "Technological Change and the Australian Constitution," *Melbourne University Law Review*, 25 (2000), http://www.austlii.edu.au/au/journals/MULR/2000/25.html.

7. The Australian Communications and Media Authority was formed in July 2005, merging the Australian Broadcasting Authority and the Australian Communications Authority. See Australian Communications and Media Authority, "The ACMA Overview," http://www.acma.gov.au/WEB/STANDARD//pc=ACMA_ORG_OVIEW.

8. Electronic Frontiers Australia, "Internet Censorship Laws in Australia," March 31, 2006, http://www.efa.org.au/Issues/Censor/cens1.html.

9. Ibid.; Office of Film and Literature Classification, "Guidelines for the Classification of Films and Computer Games," 2005, http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(CFD7369FCAE9B8F32F341DBE097801FF)~60000PB+-+Guidelines+for+the+Classification+of+Computer+Games+(Amendments+No+1)+(GN+~+Superceded+InstrumentsAMENDNO1GN22.pdf/$file/60000PB+-+Guidelines+for+the+Classification+of+Computer+Games+(Amendments+No+1)+(GN+~+Superceded+InstrumentsAMENDNO1GN22.pdf.

10. Electronic Frontiers Australia, "Internet Censorship Laws in Australia," March 31, 2006, http://www.efa.org.au/Issues/Censor/cens1.html.

11. Australian Communications and Media Authority, "Online Regulation," February 2007, http://www.acma.gov.au/web/STANDARD//pc%3DPC_90169.

12. Schedule 1, "Codes for Industry Co-regulation in Areas of Internet and Mobile Content (Pursuant to the Requirements of the Broadcasting Services Act 1992)," May 2005, http://www.acma.gov.au/acmainterwr/aba/contentreg/codes/internet/documents/iia_code.pdf.

13. Internet Industry Association, "IIA Guide for ISPs," March 23, 2006, http://www.iia.net.au/index.php?option=com_content&task=view&id=121&Itemid=33.

14. Electronic Frontiers Australia, "Internet Censorship Laws in Australia," March 31, 2006, http://www.efa.org.au/Issues/Censor/cens1.html.

15. Ibid.

16. Classification (Publications, Films and Computer Games) (Enforcement) Act 1995, §57, http://www.austlii.edu.au/au/legis/vic/consol_act/cfacga1995596/s57.html.

17. Electronic Frontiers Australia, "Internet Censorship Laws in Australia," March 31, 2006, http://www.efa.org.au/Issues/Censor/cens1.html.

18. Stephen Hutcheon, "YouTube Bans Don't Work: Internet Founder," March 8, 2007, *Sydney Morning Herald*, http://www.smh.com.au/articles/2007/03/08/1173166844770.html.

19. Ibid.

20. Stephen Deare, "ISP Level Porn Filtering Won't Work, Says Coonan," *CNet Australia*, June 15, 2006, http://www.cnet.com.au/broadband/0,239036008,240063710,00.htm.

21. *ABC News*, "Conroy Announces Mandatory Internet Filters to Protect Children," December 31, 2007, http://www.abc.net.au/news/stories/2007/12/31/2129471.htm.

22. Asher Moses, "Banned Hyperlinks Could Cost You $11,000 a Day," *The Age*, March 17, 2009, http://www.theage.com.au/news/home/technology/banned-hyperlinks-could-cost-you-11000-a-day/2009/03/17/1237054787635.html?page=fullpage#contentSwap1&page=-1/.

23. ACMA, "Restricted Access System Declaration 2007," http://www.acma.gov.au/WEB/STANDARD/pc=PC_310905.

24. Tom Corelis, "Australia Approves Mandatory Age Verification for Internet Content," *Daily Tech*, December 26, 2007, http://www.dailytech.com/Australia+Approves+Mandatory+Age+Verification+for+Internet+Content/article10137.htm.

25. ''Optus Joins ISP Net Filter Trials,'' *ITNews*, April 22, 2009, http://www.itnews.com.au/News/101538,optus-joins-isp-net-filter-trials.aspx.

26. Asher Moses, ''Filtering Out the Fury: How Government Tried to Gag Web Censor Critics,'' *Sydney Morning Herald*, October 24, 2008, http://www.smh.com.au/news/technology/biztech/government-gags-web-censor-critics/2008/10/23/1224351430987.html?page=2.

27. Andrew Hendry and Darren Pauli, '''Appalled' Opposition Hits Back at Conroy's Internet Censorship,'' *ComputerWorld*, October 24, 2008, http://www.computerworld.com.au/article/264974/appalled_opposition_hits_back_conroy_internet_censorship?pp=3&fp=4194304&fpid=1.

28. Wikileaks, ''Australia Secretly Censors Wikileaks Press Release and Danish Internet Censorship List,'' March 16, 2009, http://www.wikileaks.org/wiki/Australia_secretly_censors_Wikileaks_press_release_and_Danish_Internet_censorship_list,_16_Mar_2009/.

29. Liam Tung, ''Wikileaks Spills ACMA Blacklist,'' *ZDNet*, March 19, 2009, http://www.zdnet.com.au/news/security/soa/Wikileaks-spills-ACMA-blacklist/0,130061744,339295538,00.htm?omnRef=http://www.google.com/search?q=ACMA%20trial%20australia&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a.

30. Department of Internal Affairs: Censorship Compliance, ''Censorship and the Internet,'' http://www.censorship.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Censorship-Compliance-Censorship-and-the-Internet?OpenDocument.

31. Electronic Frontiers Australia, ''Internet Censorship: Law and Policy around the World,'' March 28, 2002, http://www.efa.org.au/Issues/Censor/cens3.html#nz.

32. Films, Videos, and Publications Act 1993, §3, http://rangi.knowledge-basket.co.nz/gpacts/reprint/text/2005/se/042se3.html.

33. Ibid.

34. Ibid.

35. Department of Internal Affairs: Censorship Compliance, ''Censorship and the Internet,'' http://www.censorship.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Censorship-Compliance-Censorship-and-the-Internet?OpenDocument.

36. Department of Internal Affairs, ''Censorship Compliance,'' December 2006, http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Censorship-Compliance-Index?OpenDocument.

37. Films, Videos, and Publications Act 1993, §23, http://rangi.knowledge-basket.co.nz/gpacts/public/text/1993/se/094se23.html.

38. InternetNZ, ''ICOP,'' May 2006, http://www.internetnz.net.nz/proceedings/tf/archive/icop05_wp_index.htm.

39. Department of Internal Affairs, Amendment Act 2005, April 2005, http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Censorship-Compliance-Amendment-Act-2005?OpenDocument.

40. Keith Manch and David Wilson, ''Objectionable Material on the Internet: Developments in Enforcement,'' Department of Internal Affairs, 2003, http://www.netsafe.org.nz/Doc_Library/

netsafepapers_manchwilson_objectionable.pdf; Electronic Frontiers Australia, ''Internet Censorship: Law and Policy around the World,'' March 28, 2002, http://www.efa.org.au/Issues/Censor/cens3.html#nz.

41. Racial Discrimination Act 1975, §18C, http://austlii.law.uts.edu.au/au/legis/cth/consol_act/rda1975202/s18c.html.

42. Galexia, ''Article: *Jones v Töben*: Racial Discrimination on the Internet,'' October 2002, http://www.galexia.com/public/research/articles/research_articles-art22.html#fn357.

43. Australian Department of Communications, Information Technology and the Arts, ''Racism and the Internet,'' November 2002, http://www.archive.dbcde.gov.au/__data/.../Racism_and_the_Internet.doc.

44. Chilling Effects, ''Google Removal Complaint: Section 18C of Australia's Racial Discrimination Act of 1975,'' May 5, 2006, http://www.chillingeffects.org/international/notice.cgi?NoticeID=4266.

45. Human Rights Act 1993, §21(1), http://www.legislation.govt.nz/act/public/1993/0082/latest/DLM304475.html.

46. Films, Videos, and Publication Act 1993, §3e, http://rangi.knowledge-basket.co.nz/gpacts/reprint/text/2005/se/042se3.html.

47. Austrade, ''The Australian–United States Free Trade Agreement,'' http://www.austrade.gov.au/AUSFTA8310/default.aspx.

48. Australian Department of Foreign Affairs and Trade, ''Intellectual Property,'' http://www.dfat.gov.au/trade/negotiations/us_fta/outcomes/08_intellectual_property.html; Australian Department of Foreign Affairs and Trade, ''A Guide to the Agreement: Intellectual Property,'' http://www.dfat.gov.au/trade/negotiations/us_fta/guide/17.html.

49. Australian Department of Foreign Affairs and Trade, ''Intellectual Property,'' http://www.dfat.gov.au/trade/negotiations/us_fta/outcomes/08_intellectual_property.html.

50. Judy Skatssoon, ''Google Warns Aust Copyright Laws Could Cripple the Internet,'' *ABC Science Online*, November 7, 2006, http://www.abc.net.au/news/newsitems/200611/s1782921.htm.

51. Ibid.

52. Jeff Garnet, ''Australian Law Could Spell Trouble for iPod Users,'' iPod Observer, November 21, 2006, http://www.ipodobserver.com/ipo/article/Australian_Law_Could_Spell_Trouble_for_iPod_Owners/.

53. Attorney General, ''Copyright Amendment Act 2006,'' December 2006, http://www.ag.gov.au/www/agd/agd.nsf/Page/Copyright_IssuesandReviews_CopyrightAmendmentAct2006.

54. Ibid.

55. Australian Copyright Council, Copyright Amendment Act 2006, January 2007, http://www.copyright.org.au/g096.pdf.

56. Asher Moses, "Copyright Ruling Puts Hyperlinking on Notice," *Sydney Morning Herald*, December 19, 2006, http://www.smh.com.au/news/web/copyright-ruling-puts-linking-on-notice/2006/12/19/1166290520771.html.

57. Ibid.

58. Allan Swann, "Entire Copyright Act to Be Scrapped," *National Business Review*, May 1, 2009, http://www.nbr.co.nz/article/entire-copyright-act-be-scrapped-101820.

59. Ministry of Economic Development, "Copyright Protection in New Zealand," November 29, 2005, http://www.med.govt.nz/templates/Page____7290.aspx.

60. Copyright (New Technologies and Performers' Rights) Amendment, §44, http://www.parliament.nz/NR/rdonlyres/5A88D15B-C4A1-42C2-AE75-9200DD87F738/51071/DBHOH_BILL_7735_40199.pdf.

61. Judith Tizard, "Digital Copyright Bill: Questions and Answers," Official Web site of New Zealand government, December 21, 2006, http://www.beehive.govt.nz/ViewDocument.aspx?DocumentID=28179.

62. Ibid.

63. Electronic Frontiers Australia, "Defamation Laws and the Internet," January 14, 2006, http://www.efa.org.au/Issues/Censor/defamation.html#2006.

64. Australian Government, Attorney General's Department, "Defamation Law Reform," http://www.ag.gov.au/www/agd/agd.nsf/Page/Defamationlawreform_Defamationlawreform.

65. Ibid.

66. Rhonda Breit, "Uniform Defamation Laws: A Fresh Start or the Same Chilling Problems?" *Australian Policy Online*, May 11, 2006, http://search.arrow.edu.au/main/redirect_to_title?identifier=oai%3Aarrow.nla.gov.au%3A120883974282815.

67. Electronic Frontiers Australia, "Defamation Laws and the Internet," January 14, 2006, http://www.efa.org.au/Issues/Censor/defamation.html.

68. *Out-Law*, "Australia Rules on Where to Sue for Internet Defamation," December 10, 2002, http://www.out-law.com/page-3184.

69. *Dow Jones and Company Inc. v. Gutnick*, December 10, 2002, http://www.austlii.edu.au/au/cases/cth/high_ct/2002/56.html.

70. Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (New York: Oxford University Press, 2006), 148.

71. Caslon Analytics, "Brown, O'Brien, and Domainz," http://www.caslon.com.au/defamationprofile10.htm#brown; Simpson Grierson, "Say No Evil: Defamation in Cyberspace," FindLaw, http://www.findlaw.com/12international/countries/nz/articles/852.html.

72. Simpson Grierson, "Say No Evil: Defamation in Cyberspace," FindLaw, http://www.findlaw.com/12international/countries/nz/articles/852.html.

73. *The University of Newlands and Anor v. Nationwide News Pty. Ltd.* [2006] N.Z.S.C. 16 SC.

74. Telecommunications (Interceptions and Access) Act 1979, §7 and §108, http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/.

75. Electronic Frontiers Australia, ''Telecommunications Privacy Laws,'' October 19, 2006, http://www.efa.org.au/Issues/Privacy/privacy-telec.html.

76. Ibid.

77. Electronic Frontiers Australia, ''Comments on the Surveillance Devices Bill 2004,'' May 18, 2004, http://www.aph.gov.au/senate/committee/legcon_ctte/completed_inquiries/2002-04/surveillance/submissions/sub8.pdf.

78. Internet Industry Association, Cybercrime Code of Practice, §7, September 2003, http://www.iia.net.au/cybercrime_code_v2.doc (accessed March 16, 2007).

79. Internet Industry Association, Cybercrime Code of Practice, §8, September 2003, http://www.iia.net.au/cybercrime_code_v2.doc (accessed March 16, 2007).

80. Telecommunications Act 1997, §282 (3), http://www.austlii.edu.au/au/legis/cth/num_reg_es/tar200232002n297457.html.

81. Green Party of Aotearoa New Zealand, ''Fact Sheet on Government Plans for E-mail Snooping and Computer Hacking on the Public,'' March 31, 2001, http://www.votegreen.org.nz/searchdocs/other4819.html.

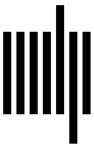
Access Controlled

The Shaping of Power, Rights, and Rule in Cyberspace

Edited by: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan L. Zittrain

Citation:

Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace
Edited by: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan L. Zittrain
DOI: 10.7551/mitpress/8551.001.0001
ISBN (electronic): 9780262266031
Publisher: The MIT Press
Published: 2010



The MIT Press

For information about special quantity discounts, please email special_sales@mitpress.mit.edu

This book was set in Stone Serif and Stone Sans on 3B2 by Asco Typesetters, Hong Kong.

Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Access controlled : the shaping of power, rights, and rule in cyberspace / edited by Ronald Deibert . . . [et al.] ; foreword by Miklos Haraszti.
p. cm. — (Information revolution and global politics)
Report from the OpenNet Initiative.
Includes bibliographical references and index.
ISBN 978-0-262-01434-2 (hardcover : alk. paper) — ISBN 978-0-262-51435-4 (pbk. : alk. paper)
1. Cyberspace—Government policy. 2. Internet—Government policy. 3. Computers—Access control. 4. Internet—Censorship. I. Deibert, Ronald. II. OpenNet Initiative.
HM851.A254 2010
005.8—dc22 2009049632

10 9 8 7 6 5 4 3 2 1