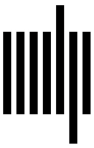
Access Denied

The Practice and Policy of Global Internet Filtering

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

Citation:

Access Denied: The Practice and Policy of Global Internet Filtering
Edited by: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan L. Zittrain
DOI: 10.7551/mitpress/7617.001.0001
ISBN (electronic): 9780262255998
Publisher: The MIT Press
Published: 2008



The MIT Press

Internet Filtering in
Australia and New Zealand

Introduction

Australia maintains some of the most restrictive Internet policies of any Western nation, while its neighbor, New Zealand, is less rigorous in its Internet regulation. Without any explicit protection of free speech in its constitution,[1] the Australian government has used its "communications power" delineated in the constitution to regulate the availability of offensive content online,[2] endowing a government entity with the power to issue take-down notices for Internet content hosted within the country. A number of state and territorial governments in Australia have also 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 also promotes and finances an "opt-in" filtering program, in which Internet users voluntarily accept filtering software that blocks offensive content hosted outside of the country. At present there are no plans for a countrywide Internet service provider (ISP)-level filtering regime, though Australia's handling of hate speech, copyright, defamation, and security signals the government's desire to increase the scope of its Internet regulation.

New Zealand by contrast is less strict in its Internet regulation. 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 it being illegal in both countries). Furthermore, the government 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. Although New Zealand Internet copyright policies have not yet been formalized, its defamation and security policies are fairly similar to Australia's.

Overall, however, Australia maintains a stricter regime of Internet censorship and regulation than New Zealand and much of the Western world, though not at the level of the more repressive governments that ONI has studied.

Offensive content

Australian and New Zealand approaches to offensive content on the Internet are somewhat similar in structure, in that they both rely on classifications systems and entities with the power to investigate online content. But their approaches are very different 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 the 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."[4] With no explicit constitutional protection of free speech, 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)[5] 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.[6]

Web content that is hosted in Australia may be removed by 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:

- R18—Contains content that is likely to be disturbing to those under eighteen. This content is not prohibited on domestic hosting sites if there is an age-verification system certified by the ACMA in place.
- X18—Contains nonviolent sexually explicit content between consenting adults. This content may be subject to ACMA takedown provisions if hosted on domestic servers.
- RC—Contains content that is Refused Classification (child pornography, fetish, detailed instruction on crime, and so on)[7] and is prohibited on Australian-hosted sites.

The classification system chosen for Internet content is not the publications classification system but the more restrictive standard used for films. As a result, some content allowable offline is banned when brought online.[8]

Once the determination has been made that content hosted within Australia is prohibited, the ACMA issues a takedown notice to the Internet Content Host (ICH). It is not illegal for the ICH to host prohibited content, but legal action could be taken against it by the government if it does not comply with the take-down 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 sites in their filters.[9] To obtain certification, these certified "Family Friendly Filters" must agree to keep lists of prohibited sites confidential.[10] ISPs are then required to offer a Family Friendly Filter to all of their customers, though customers are not required to accept them.[11] As a result, content taken down in Australia could be posted outside of 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 site taken down has moved to the United States, even keeping its URL and ".au" domain. It is not known how many sites have moved overseas in this fashion.[12]

States and territories 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."[13] The state of Victoria, for example, in §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."[14] There is not complete 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.[15]

Beyond its regulation of online content, the Commonwealth is implementing new Internet filtering initiatives. In June 2006 the Australian government announced an AU$116.6 million initiative called "Protecting Australian Families Online." Of this, AU$93.3 million will be spent over three years to provide all families with free Web filters, though they will still be optional. Further, the National Library of Australia is now required to use Web filters on all of its computers. All other libraries are to be provided with free Web filters and encouraged to use them on their computers as well.[16] Finally, perhaps in a nod to elements of the government—especially members of the Labor Party—pushing for a system like Cleanfeed in the United Kingdom, the government will be testing an ISP-level blocking system in Tasmania. The Minister for Communications, Information Technology and the Arts, Helen Coonan, however, remains opposed to implementing this system on a countrywide basis.[17]

In a related development, all mainland states in Australia recently banned access to YouTube over school networks because of a video uploaded depicting a seventeen-year-old Australian girl being abused, beaten up, and humiliated by a group of young people. Eight youths have been charged in connection with the assault.[18] The blocking has continued to worsen rifts between state schools and some nonstate schools, such as Melbourne Grammar School, which have chosen to protect free speech and allow unfiltered access to the Internet.[19]

New Zealand, on the other hand, does not have any government legislation directly regulating Internet content.[20] Officials have claimed, however, that the Films, Videos, and Publications Classification Act of 1993, which defines "objectionable" material, covers Internet materials as well.[21] 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.[22] Specifically listed is 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 dehumanising conduct or sexual conduct; or bestiality; or acts of torture or the infliction of extreme violence or extreme cruelty."[23] There is also a decision-making 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.[24] This law has formed the basis of the Department of Internal Affairs' (DIA) enforcement of Internet censorship in the country.

Like Australia's ACMA, the DIA "proactively" investigates potentially banned material[25] and

submits any such material not already classified to the Office of Film and Literature Classification for a ruling.[26] This office then classifies the material as "unrestricted," "objectionable," or "objectionable" except in certain circumstances of restricted access or for "educational, professional, scientific, literary, artistic, or technical purposes."[27]

Unlike in Australia, however, there is no explicit legal mechanism for the take-down of objectionable material. Instead, the nonprofit InternetNZ is in the process of establishing an industrywide code of conduct that would require its signers to agree not to host illegal content.[28] 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 NZ$50,000 fine.[29] According to various sources, the DIA has almost completely focused its enforcement of Internet censorship on child pornography.[30]

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."[31]

Australian courts applied this law to the Internet for the first time in October 2002 in the *Jones v. Toben* case. Jeremy Jones and the Executive Council of Australian Jewry brought a lawsuit against Frederick Toben, the director of the Adelaide Institute, because of material on Toben'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 §18C of the Racial Discimination Act 1975 (quoted above) and called for the material to be removed from the Internet.[32]

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.[33] 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).[34] This may be indicative of a new notice-based system taking form.

New Zealand, on the other hand, has both explicit prohibition of discrimination based on race, religion, age, disability, sexual orientation, and so on in §21(1) of the Human Rights Act 1993,[35] as well as 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 §21(1) of the

Human Rights Act 1993"[36] in §3e of the Films, Videos and Publication Classifications Act 1993. The DIA uses these statutes to pursue investigations into potentially discriminatory material.

Copyright

Australia is applying copyright law to the Internet in a vigorous attempt to expand its role in limiting copyright infringement. New Zealand, on the other hand, is more slow-moving and has yet to enact legislation directly relevant to Internet copyright.

Australia's copyright laws underwent significant overhaul following the acceptance of the Australian-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.[37] Some of the relevant requirements included:

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, and
5. increasing the length of copyright to life + seventy years from its previous level of life + fifty years.[38]

Most of these provisions were implemented in the US Free Trade Agreement Implementation Act 2004,[39] though new regulations in response to requirement (3) were recently implemented in the Copyrights Amendment Act 2006.[40]

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 to, as ABC Science Online reports, "keep up with the rapidly changing digital landscape."[41] 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 site. This would "condemn the Australian public to the pre-Internet era," Google argued.[42] Other critics contended that the proposed amendments would make possession of an iPod or other music-listening device designed to play MP3s illegal, and uploading a video of yourself singing along to a pop song a crime.[43]

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),[44] 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."[45] However, this does not appear to offer the exception that Google sought.

Overall, though, the amendments allow for increased exceptions to the copyright laws to establish more realistic fair use of copyrighted material, such as "time-shifting, format-shifting and space-shifting" (e.g., 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.[46]

The Australian judiciary has been active in setting precedents in copyright enforcement online. 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.[47] 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."[48]

In New Zealand, there is no legislation in effect that explicitly relates copyright law to the Internet. Current New Zealand copyright law is contained within the Copyright Act 1994, which makes exceptions for time-shifting of television programs but none for format- or space-shifting of content. In addition, copyright is set at life + fifty years.[49]

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,[50] 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."[51] 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.[52]

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 Australia courts' example, have controversially expanded their jurisdiction in defamation suits to online materials hosted outside of their borders.

Defamation in Australia, except for a small range of cases, is handled through state and territorial law.[53] And until December 2005, states and territories maintained largely nonuniform codes of defamation.[54] 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.[55] Since defamation laws in Australia 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.[56] 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.[57]

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) are 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.[58]

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."[59] The parties eventually settled for AU$180,000 in damages and AU$400,000 in legal fees."[60]

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, CEO 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.[61] 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.[62]

In addition the New Zealand courts have followed in Australia's example in determining the jurisdiction for defamation suits over online content hosted in a foreign country. Ironically enough, 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 essentially eschewed the United States' rule of "single publication" and more closely aligned New Zealand defamation policy with Australia.[63]

Security

Both Australia and New Zealand have taken steps toward greater Internet security in their countries, 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.[64] 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).[65]

The second relevant law is the Surveillance Devices Act 2004, which significantly increases the authority of law enforcement to install surveillance devices such as key-stroke recorders under newly created "surveillance device warrants."[66] 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.[67]

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 email information, were to be kept for six months after creation of the data.[68] Law enforcement could request this information using the certificate system set up in the Telecommunications Act 1997,[69] which allows private information to be disclosed if "an authorised officer of a criminal law-enforcement agency has certified that the disclosure is reasonably necessary for the enforcement of the criminal law."[70] The code was skewered by privacy advocates,[71] and it is still listed as "not yet ratified" and "in public consultation" on the IIA's Web site, even though it was released four years ago.[72]

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, Security Intelligence Service, and the Government Communications Security Bureau acting under interception warrants as described by the Crimes Act 1961. As Keith Locke of the Green Party points out, however, these warrants "can be quite broad in their application and cover a class of people."[73]

Conclusion

Australian laws and policies toward the Internet are restrictive relative to similar Western countries, while New Zealand is less stringent. The Australian government has instituted a strict takedown regime for offensive content, and various states and territories have made distribution of said 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. So far, the government has resisted calls to implement ISP-level blocking of offensive content on a countrywide basis, though there is significant political backing to implement one.

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

Overall, though, Australia's Internet censorship regime is strikingly severe relative to both its neighbor and similar Western states. It is not, however, at the level of the most repressive regimes that ONI has examined.

Author: Evan Croen

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. See Australian Constitution, §51(v), http://scaleplus.law.gov.au/html/pasteact/1/641/0/PA000700.htm.
3. Electronic Frontiers Australia, "Internet censorship laws in Australia," March 31, 2006, http://www.efa.org.au/Issues/Censor/cens1.html.
4. Australian Constitution, §51(v), http://scaleplus.law.gov.au/html/pasteact/1/641/0/PA000700.htm.

5. The Australian Communications and Media Authority was formed in July 2005, merging the Australian Broadcasting Authority and the Australian Communications Authority. See ACMA Overview, http://www.acma.gov.au/WEB/STANDARD//pc=ACMA_ORG_OVIEW.
6. Electronic Frontiers Australia, "Internet censorship laws in Australia," March 2006, http://www.efa.org.au/Issues/Censor/cens1.html.
7. Ibid.; Office of Film and Literature Classification, Guidelines for the Classification of Films and Computer Games, 2005, http://www.oflc.gov.au/resource.html?resource=62&filename=62.pdf.
8. Electronic Frontiers Australia, "Internet censorship laws in Australia," March 2006, http://www.efa.org.au/Issues/Censor/cens1.html.
9. Australian Communications and Media Authority, "Internet regulation," February 2007, http://www.acma.gov.au/web/STANDARD//pc%3DPC_90169.
10. 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.
11. IIA Guide for ISPs, March 2006, http://www.iia.net.au/index.php?option=com_content&task=view&id=121&Itemid=33.
12. Electronic Frontiers Australia, "Internet censorship laws in Australia," March 31, 2006, http://www.efa.org.au/Issues/Censor/cens1.html.
13. Ibid.
14. Classification (Publications, Films and Computer Games) (Enforcement) Act 1995, §57, http://www.austlii.edu.au/au/legis/vic/consol_act/cfacga1995596/s57.html.
15. Electronic Frontiers Australia, "Internet censorship laws in Australia," March 31, 2006, http://www.efa.org.au/Issues/Censor/cens1.html.
16. Senator Helen Coonan, "$116.6 million to protect Australian families," June 2006, http://www.minister.dcita.gov.au/media/media_releases/$116.6_million_to_protect_australian_families_online.
17. Stephen Deare, "ISP level porn filtering won't work, says Coonan," June 2006, http://www.cnet.com.au/broadband/0,239036008,240063710,00.htm.
18. Stephen Hutcheon, "YouTube bans don't work: Internet founder," March 2007, http://www.stuff.co.nz/3986172a11275.html.
19. Ibid.
20. InternetNZ, "Internet governance in NZ," http://www.internetnz.net.nz/net-in-nz/governance.
21. Electronic Frontiers Australia, "Internet censorship: Law and policy around the world," March 28, 2002, http://www.efa.org.au/Issues/Censor/cens3.html#nz.
22. Films, Videos, and Publications Act 1993, §3, http://rangi.knowledge-basket.co.nz/gpacts/reprint/text/2005/se/042se3.html.
23. Ibid.
24. Ibid.
25. Department of Internal Affairs, Censorship and the Internet, November 2006, http://www.censorship.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Censorship-Compliance-Censorship-and-the-Internet?OpenDocument.
26. Department of Internal Affairs, Censorship Compliance, December 2006, http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Censorship-Compliance-Index?OpenDocument.
27. Films, Videos, and Publications Act 1993, §23, http://rangi.knowledge-basket.co.nz/gpacts/public/text/1993/se/094se23.html.
28. InternetNZ, "ICOP," May 2006, http://www.internetnz.net.nz/issues/current-issues/ICOP.
29. Department of Internal Affairs, Amendment Act of 2005, April 2005, available at http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Censorship-Compliance-Amendment-Act-2005?OpenDocument.
30. Keith Manch and David Wilson, "Objectionable material on the Internet: Developments in enforcement," 2003, 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.
31. Racial Discrimination Act 1975, §18C, http://austlii.law.uts.edu.au/au/legis/cth/consol_act/rda1975202/s18c.html.
32. Galexia, "Article: Jones v Toben: Racial discrimination on the Internet," Oct 2002, http://www.galexia.com/public/research/articles/research_articles-art22.html#fn357.
33. Australian Department of Communications, Information Technology and the Arts, "Racism and the Internet," November 2002, www.dcita.gov.au/__data/assets/word_doc/10892/Racism_and_the_Internet.doc.
34. Chilling Effects, "Google removal complaint: §18C of Australia's Racial Discrimination Act of 1975," May 2006, http://www.chillingeffects.org/international/notice.cgi?NoticeID=4266.
35. Human Rights Act 1993, §21(1), http://www.legislation.govt.nz/browse_vw.asp?content-set=pal_statutes.
36. Films, Videos and Publication Act 1993, §3e, http://rangi.knowledge-basket.co.nz/gpacts/reprint/text/2005/se/042se3.html.
37. Austrade, "The Australian-United States Free Trade Agreement in brief," http://www.fta.gov.au/ArticleDocuments/AUSFTA Client Brochure_Final_200606.pdf.aspx.

38. 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.
39. Australian Copyright Council, Free Trade Agreement Amendments, January 2006, http://www.copyright.org.au/publications/G085.pdf.
40. Australian Department of Foreign Affairs and Trade, Intellectual Property, http://www.dfat.gov.au/trade/negotiations/us_fta/outcomes/08_intellectual_property.html.
41. 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.
42. Ibid.
43. Associated Press, "Proposed changes to Australian copyright laws could make iPod user into criminals," November 21, 2006, http://www.iht.com/articles/ap/2006/11/21/technology/AS_TEC_Australia_Copyright_Crime.php.
44. The Attorney-General, Copyright Amendment Bill 2006: Frequently Asked Questions, December 2006, http://www.ag.gov.au/agd/WWW/MinisterRuddockHome.nsf/Page/RWPC7B0742318EF6A58CA25723B008145FC.
45. Copyright Amendment Act 2006, http://www.comlaw.gov.au/ComLaw/Legislation/Act1.nsf/0/5A32BBA137EC7020CA2572440000E793/$file/1582006.pdf.
46. Australian Copyright Council, Copyright Amendment Act 2006, January 2007, http://www.copyright.org.au/g096.pdf.
47. 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.
48. Ibid.
49. Ministry of Economic Development, Copyright Protection in New Zealand, November 29, 2005, http://www.med.govt.nz/templates/Page____7290.aspx.
50. 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.
51. Judith Tizard, "Digital copyright bill: Questions & answers," Official Web site of New Zealand government, December 21, 2006, http://www.beehive.govt.nz/ViewDocument.aspx?DocumentID=28179.
52. Ibid.
53. Electronic Frontiers Australia, "Defamation laws and the Internet," January 14, 2006, http://www.efa.org.au/Issues/Censor/defamation.html#2006.
54. The Attorney-General, "Belated state defamation laws," December 15, 2005, http://www.ag.gov.au/agd/WWW/MinisterRuddockHome.nsf/Page/Media_Releases_2005_Fourth_Quarter_15_December_2005_-_Belated_State_defamation_laws_-_2372005.
55. Ibid.
56. Rhonda Breit, "Uniform defamation laws: A fresh start or the same chilling problems?" The Brisbane Institute, May 11, 2006, http://www.brisinst.org.au/resources/brisbane_institute_defamation.html.
57. Electronic Frontiers Australia, "Defamation laws and the Internet," January 14, 2006, http://www.efa.org.au/Issues/Censor/defamation.html.
58. OUT-LAW News, "Australia rules on where to sue for internet defamation," December 10, 2002, http://www.out-law.com/page-3184.
59. *Dow Jones & Company Inc. v. Gutnick,* December 10, 2002, http://www.austlii.edu.au/au/cases/cth/high_ct/2002/56.html.
60. Jack Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World.* New York: Oxford University Press, 2006, p. 148.
61. Caslon Analytics, "Brown, O'Brien, and Domainz," http://www.caslon.com.au/defamationprofile10.htm#brown, (accessed March 16, 2007); FindLaw, "Say No Evil: Defamation in Cyberspace," http://www.findlaw.com/12international/countries/nz/articles/852.html, (accessed March 16, 2007).
62. FindLaw, "Say No Evil: Defamation in Cyberspace," http://www.findlaw.com/12international/countries/nz/articles/852.html,(accessed March 16, 2007)
63. Sarah Harrison, "Overseas website caught by New Zealand defamation laws," AJ Park, November 1, 2004, http://www.ajpark.co.nz/library/2005/03/oseas_website_defamation_laws.php.
64. Telecommunications (Interceptions and Access) Act 1979, §7 and §108, http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/.
65. Electronic Frontiers Australia, "Telecommunications privacy laws," October 19, 2006, http://www.efa.org.au/Issues/Privacy/privacy-telec.html.
66. Ibid.
67. Electronic Frontiers Australia, "EFA comments on Surveillance Devices Bill 2004," May 18, 2004, http://www.aph.gov.au/senate/committee/legcon_ctte/completed_inquiries/2002-04/surveillance/submissions/sub8.pdf.
68. Internet Industry Association, Cybercrime Code of Practice, §7, September 2003, www.iia.net.au/cybercrime_code_v2.doc, (accessed March 16, 2007).
69. Ibid, §8.

70. Telecommunications Act 1997, §282 (3), http://www.comlaw.gov.au/comlaw/legislation/act-compilation1.nsf/0/D22A9.DC08193D6D8CA25726D007B99E4/$file/Tele1997_Version2_WD02.pdf
71. Steven Dreare, "Privacy advocates rip into ISP cybercrime code," *PCWorld,* August 21, 2003, http://www.crime-research.org/news/2003/08/Mess2102.html.
72. Internet Industry Association, Cybercrime Code of Practice, http://www.iia.net.au/index.php?option=com_content&task=category&sectionid=3&id=22&Itemid=33, (accessed March 16, 2007).
73. Keith Locke, Fact Sheet on Government Plans for E-mail Snooping and Computer Hacking on the Public, Green Party of Aotearoa New Zealand, March 31, 2001, http://www.votegreen.org.nz/searchdocs/other4819.html.

For information about special quantity discounts, please e-mail special_sales@mitpress.mit.edu.

This book was set in Swis721 on 3B2 by Asco Typesetters, Hong Kong.
Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Access denied : the practice and policy of global Internet filtering / edited by Ronald Deibert . . . [et al.].
p. cm. — (The information revolution & global politics series)
Includes bibliographical references and index.
ISBN 978-0-262-54196-1 (pbk. : alk. paper) — ISBN 978-0-262-04245-1 (hardcover : alk. paper)
1. Computers—Access control. 2. Internet—Censorship. 3. Internet—Government policy. I. Deibert, Ronald.
QA76.9.A25.A275 2008
005.8—dc22 2007010334

10 9 8 7 6 5 4 3 2 1