FILTERING IN OZ: AUSTRALIA'S FORAY INTO INTERNET CENSORSHIP

DEREK E. BAMBAUER[*]

ABSTRACT

Australia's decision to implement Internet censorship using technological means creates a natural experiment: it can become the first Western democracy to mandate filtering legislatively and to retrofit it to a decentralized network. But are the proposed restrictions legitimate? The new restraints derive from the Labor Party's pro-filtering electoral campaign, though minority politicians have considerable influence over policy. The country has a well-defined statutory censorship system that may, however, be undercut by relying on foreign and third-party lists of sites to be blocked. While Australia is open about its filtering goals, the government's transparency about what content is to be blocked is poor. Initial tests show that how effective censorship is at filtering prohibited content—and only that content—will vary based on what method ISPs use. Though Australia's decision-makers are formally accountable, efforts to silence dissenters, outsourcing of blocking decisions, and filtering's inevitable transfer of power to technicians undercut accountability. This Article argues that Australia represents a shift by Western democracies towards legitimating Internet filtering and away from robust consideration of the alternatives available to combat undesirable information.

[*] Assistant Professor of Law, Brooklyn Law School. A.B, Harvard College; J.D., Harvard Law School. The Author thanks Jelena Kristic and Brad Reid for expert research assistance. Thanks for helpful suggestions and discussion are owed to Sarah Abramowicz, Miriam Baer, Irene Graham, Dan Hunter, Alana Maurushat, Jason Mazzone, Sam Murumba, Mark Newton, Dana Brakman Reiser, John Selby, Nic Suzor, Yane Svetiev, David Vaile, the participants at the University of New South Wales Internet Filtering and Censorship Forum, and the participants at Computers, Freedom & Privacy 2009. The Author welcomes comments at derek.bambauer@brooklaw.edu. This Article is based in part on the Author's work as a Research Fellow at the Berkman Center for Internet & Society at Harvard Law School with the OpenNet Initiative.

TABLE OF CONTENTS

1. INTRODUCTION

Australia's decision to impose mandatory Internet censorship through technology—"filtering," as it is known in cyberlaw—puts the country at the forefront of the spread of this practice from authoritarian regimes such as China and Iran to Western democratic nations.[1] This Article describes Australia's proposed filtering system in its technical and legal aspects and assesses both the legitimacy of this censorship and its likely effects on debates over online information controls.[2] In short, while much depends on how Australia implements restrictions, current plans raise concerns about the transparency and accountability of the government's efforts, and may create a clash between efforts to block unlawful content and to expand broadband access. Moreover, the dynamics created by filtering may inevitably lead Australia to expand the scope of material blocked. Australia's efforts create a fascinating experiment in Internet censorship by Western democracies.

Australia is not the first Western country to implement Internet censorship, but its proposed system is unique in several important respects. First, the current government, led by the Labor Party,

[1] *See generally* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING (Ronald Deibert et al. eds. 2008). I use the terms "filtering" and "censorship" interchangeably. *See generally* OPENNET INITIATIVE, ABOUT FILTERING, http://opennet.net/about-filtering (last visited Dec. 5., 2009); Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653 (2003).

[2] Two cautions are in order. First, Australia's filtering system has yet to be implemented and its configuration and details may change. Second, the author is an American attorney, not an Australian one, which inevitably affects the Article's analysis.

made filtering a key aspect of its program during its electoral campaigning.[3] The government thus has a tenable claim to a democratic mandate for Internet censorship. Second, Australia plans to mandate censorship by law, rather than through informal pressure on Internet Service Providers ("ISPs") (as the United Kingdom has done)[4] or through partial measures aimed at intermediaries such as search engines (as France and Germany have done).[5] This is the first time that a Western democracy will require, through formal statute, ISPs to block users from accessing certain materials online. Third, the criteria by which sites will be designated for blocking remain opaque and uncertain; the government has vacillated between focusing on child pornography sites[6] and suggesting that other topics, such as hate speech and violence, could also be banned.[7] Most Western nations that censor the Net specify closely the material that is blocked. Finally, the government appears willing to trade performance degradation to block suspect sites; a pilot test of filtering found decreases in access speeds from 2% to 86%.[8] This creates tension between Labor's

[3] Andrew Hendry & Darren Pauli, *"Appalled" Opposition Hits Back at Conroy's Internet Censorship*, COMPUTERWORLD, Oct. 24, 2008, http://www.computerworld.com.au/index.php/id;879301684;fp;4194304;fpid;1 (quoting "shadow broadband minister" Senator Nick Minchin who observed that "Labor went to the election and won on the basis of this, frankly, very heavy-handed one-size-fits-all ISP-based content filter").

[4] *See* Frank Fisher, *Caught in the Web*, THE GUARDIAN, Jan. 17, 2008, *available at* http://www.guardian.co.uk/commentisfree/2008/jan/17/caughtintheweb (detailing the UK government's effort to suppress certain content by demanding that ISPs voluntarily opt into a system that has not been discussed or debated by the legislature).

[5] *See* OpenNet Initiative, Europe, http://opennet.net/research/regions/europe (last visited Dec. 3, 2009) (observing that both France and Germany have worked with search engines to remove illegal content and hate speech).

[6] *See, e.g.*, STEPHEN CONROY, LABOR'S PLAN FOR CYBER-SAFETY 5 (2007), *available at* http://www.alp.org.au/download/now/labors_plan_for_cyber_safety.pdf (stating "Labor's ISP policy will prevent Australian children from accessing any content that has been identified as prohibited by [the Australian Communications and Media Authority], including sites such as those containing child pornography and X-rated material").

[7] *See Senator Conroy Expands Reach of Net Filters to "Unwanted Content,"* ITNEWS AUSTRALIA, Nov. 13, 2008, http://www.itnews.com.au/News/88908,senator-conroy-expands-reach-of-net-filters-to-unwanted-content.aspx (noting that net filters will be expanded to reach "unwanted content").

[8] AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY, CLOSED ENVIRONMENT TESTING OF ISP-LEVEL INTERNET CONTENT FILTERING 41, 62–68 (June 2008), *available at* http://www.acma.gov.au/webwr/_assets/main/lib310554/isp-level_internet_content_filtering_trial-report.pdf.

policy goals, as increasing broadband access and access speeds are core tenets of the government's platform.[9]

The new government's Internet censorship proposals have been controversial, spawning street protests,[10] online petitions,[11] opposition from Internet industry groups,[12] and critical press coverage.[13] Nonetheless, Australia is forging ahead with plans to test filtering.[14]

Is Australia's proposed Internet filtering legitimate? Assessing censorship normatively is tricky; the most common method is to examine what content is proscribed and then articulate a position based on one's view of that material. However, the Internet is local where censorship is concerned. Different countries, even democratic ones, make varying decisions.[15] It may be legitimate for France to ban hate speech online and for the United States to permit it, even though the targeted content is the same. In a separate Article, I propose moving from an ends-based analysis (examining what content is filtered) to a process-based methodology examining how censorship decisions are made and implemented.[16]

To assess legitimacy, this process-based framework asks four questions. First, is a country *open* about its Internet censorship and why it restricts information? Second, is the state *transparent* about

[9] AUSTRALIAN LABOR PARTY, NATIONAL PLATFORM AND CONSTITUTION 23 (2007), *available at* http://www.alp.org.au/platform/index.php.

[10] *See* Darren Pauli, *Anti Internet Filtering Rebels Hit the Streets*, COMPUTERWORLD, Dec. 3, 2008, http://www.computerworld.com.au/article/269615/anti_content_filtering_rebels_take_streets?fp=16&fpid=1 (describing protests that were arranged in Australia's capital cities by members from organizations including the Electronic Freedom Project and the Digital Liberty Coalition).

[11] Computerworld, Save the Internet!, http://www.computerworld.com.au/user/login?destination=hands_off_the_internet (last visited Dec. 2, 2009).

[12] Hendry & Pauli, *supra* note 3.

[13] *See, e.g.*, Jennifer Dudley-Nicholson, *Australia's Compulsory Internet Filtering "Costly, Ineffective,"* THE COURIER-MAIL, Oct. 29, 2008, *available at* http://www.news.com.au/technology/story/0,25642,24569656-5014239,00.html.

[14] *See* Fran Foo, *ISP Filtering Gathers Pace*, AUSTRALIAN IT, Feb. 12, 2009, *at* http://www.australianit.news.com.au/story/0,24897,25043812-15306,00.html (noting ISPs were beginning to install their testing equipment).

[15] As John Perry Barlow noted, "in Cyberspace, the First Amendment is a local ordinance." John Perry Barlow, *Leaving the Physical World*, http://w2.eff.org/Misc/Publications/John_Perry_Barlow/HTML/leaving_the_physical_world.html (last visited Dec. 3, 2009).

[16] Derek E. Bambauer, *Cybersieves*, 59 DUKE L.J. 377 (2009).

what material it filters and what it leaves untouched? Third, how *narrow* is filtering: how well does the content that is actually blocked—and not blocked—correspond to those criteria? Finally, to what degree are citizens and Internet users able to participate in decision-making about these restrictions, such that censors are *accountable*?[17] Legitimate censorship is open, transparent about what is banned, effective yet narrowly targeted, and responsive to the preferences of each state's citizens.

The remainder of this Article explores the political, legal, and technological context of Australia's Internet filtering plans in Sections 2, 3, and 4; assesses the legitimacy of the proposed program using the new process-based methodology in Section 5; and concludes with an initial evaluation of what this move means for larger debates around online information restrictions.

2. POLITICAL CONTEXT

Australia's shift from voluntary filtering through software installed on individual computers to mandatory, ISP-based censorship resulted from a change in government. The Labor Party replaced the Liberal Party in power, but with a key weakness: its legislative program depended upon support from minority parties to pass in Australia's Senate. One of these parties, Family First, and its single Senator have pushed Labor to expand the scope of content filtered, despite substantial political opposition to the program.

In November 2007, the Labor Party, led by Kevin Rudd, defeated the ruling Liberal Party of John Howard.[18] While one issue in the campaign was Australia's participation in the conflict in Iraq,[19] Labor also included Internet policy topics in its platform, such as expanding broadband access and blocking sites with illegal material.[20] The filtering proposal, which was released late in the

[17] *Id.*

[18] Rohan Sullivan, *Bush Ally Howard Defeated in Australia*, WASH. POST, Nov. 25, 2007, at A17.

[19] Tim Johnston, *Tough Race in Australia for Supporter of Bush*, N.Y. TIMES, Nov. 23, 2007, at A24.

[20] *See* AUSTRALIAN LABOR PARTY, *supra* note 9, at 278 ("Labor is committed to improving the access of all Australians . . . to the benefits of broadband connectivity . . . [and] supports a requirement for internet service providers to offer a filtered 'clean feed' internet service to all households, schools and other public internet points accessible by children"). *See also* Press Release, Senator

campaign,[21] built on Labor's plan from March 2006 to mandate that "clean feed" Internet access be offered to all schools, households, and public access points available to children.[22] The Liberal Party, in contrast, advanced a filtering program, NetAlert, based on offering free software to parents and families,[23] although the Howard government did order a test of ISP-based filtering that the new Rudd government continued.[24]

During the campaign, Stephen Conroy, Labor's shadow Minister for Communications and Information Technology, promulgated a detailed plan for cyber-safety that stated Labor would require "Internet Service Providers (ISPs) [to] filter out content that is identified as prohibited by the Australian Communications and Media Authority (ACMA)," and that the "ACMA 'blacklist' will be made more comprehensive to ensure that children are protected from harmful and inappropriate material."[25] The plan criticized the Howard government's program offering free filtering software to parents, noting that a 16-year-old (known as "The Porn Cracker")[26] was able to hack the software to bypass it.[27] Moreover, despite a $22 million[28]

Stephen Conroy, Minister Welcomes Advances in Internet Filtering Technology (July 28, 2008), http://www.minister.dbcde.gov.au/media/media_releases /2008/060 (releasing the findings of reports that tested the current effectiveness of commercial Internet Service Providers filtering products).

[21] The Last Modified date on the file containing the Cyber-Safety Plan is Nov. 19, 2007; elections were held on Nov. 24, 2007. CONROY, *supra* note 6. *See* Stilgherrian, *ACS Filter Report Just What Conroy Needs*, ZDNET AUSTRALIA, Oct. 14, 2009, http://www.zdnet.com.au/insight/security/soa/ACS-filter-report-just-what-Conroy-needs/0,139023764,339299029,00.htm (describing the Plan as "thrown together in the last few weeks before the November 2007 election, well after the rest of Labor's policies had been published").

[22] Press Release, Kim Beazley, Labor's Plan to Protect Kids From Internet Pornography (Mar. 21, 2006), http://web.archive.org/web/20060422120043 /http://www.alp.org.au/media/0306/msloo210.php.

[23] *See New NetAlert—Proecting Australian Families Online Initiative Launched*, ACMASPHERE (ACMA) Sept. 2007, *available at* http://www.acma.gov.au/webwr /_assets/main/lib310211/acmasphere%20issue%2023.pdf.

[24] *See* AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY, *supra* note 8.

[25] CONROY, *supra* note 6, at 2.

[26] *See* Tom Wood, *The Wood Verdict*, http://thewoodverdict.blogspot.com/ (the "Porn Cracker's" blog). *See also* Nick Higginbottom & Ben Packham, *Student Cracks Government's $84m Porn Filter*, HERALD SUN, Aug. 26, 2007 (on file with U. PA. J. INT'L L.) (reporting that the "Porn Cracker" was able to hack the software in thirty minutes).

[27] CONROY, *supra* note 6, at 4. *See also* Meredith Booth, *Adelaide Firm to Benefit as Businesses Tighten the Net*, THE ADVERTISER, Nov. 11, 2008, at 37 (noting that

advertising budget, the NetAlert program[29] achieved only 10% of the 1.4 million software downloads initially projected by the government.[30] The Department of Broadband, Communications, and the Digital Economy estimated that only 29,000 of those downloads (2% of the target figure) were actually deployed and in use.[31] Labor successfully portrayed NetAlert's paucity of use as resulting from a failure of government rather than from a lack of public interest.

After its victory at the polls, the new Labor government moved to implement its plan to prevent access to prohibited material online. In its initial budget, the Rudd government allocated over $128 million for cyber safety and law enforcement,[32] with over $44 million dedicated to filtering.[33] The government's focus for online restrictions slowly broadened from its campaign focus on the ACMA blacklist to blocking content perceived as harmful more generally. Conroy—now Minister for Broadband, Communications, and the Digital Economy—claimed that filters will block up to 10,000 Web sites.[34] The Labor government's proposal has proved controversial, drawing opposition from Internet industry groups (including Netchoice and the System Administrators Guild of Australia),[35] free speech organizations (including Electronic Frontiers Australia),[36] newspapers and other media outlets,[37] librarians,[38] and even some children's groups (such

NetFox, a tool that filters in real time, was forecasting small business demand for its product this year will boom).

[28] Currency figures are in Australian dollars unless noted otherwise.

[29] Australian Government, NetAlert, http://www.netalert.gov.au/ (last visited Dec. 3, 2009).

[30] Andrew Colley, *Costs and Lack of Enthusiasm Threaten Free Net Nasty Blocking Plan*, AUSTRALIAN, Feb. 26, 2008, at 29.

[31] Health Gilmore, *Web Porn Software Filter Takes Biggest Hit*, SUN HERALD (Sydney), Feb. 17, 2008, at 40.

[32] Glenn Mulcaster, *Opposition Rises to Internet Filter*, THE AGE (Melbourne), Nov. 11, 2008, at 5.

[33] Samela Harris, Op-Ed., *The Hand That's On Your Mouse . . . and Why It Will Make Your Internet a Whole Lot Slower*, ADVERTISER, Oct. 28, 2008, at 19.

[34] Graham Clark, *Seven Days*, COURIER-MAIL, Nov. 15, 2008, at 54.

[35] Mulcaster, *supra* note 32.

[36] Electronic Frontiers Australia, *Labor's Mandatory ISP Internet Blocking Plan*, http://www.efa.org.au/censorship/mandatory-isp-blocking/ (last visited Dec. 3, 2009).

[37] *See, e.g.*, Editorial, *Flawed Plan for Internet Control*, CANBERRA TIMES, Jan. 3, 2008, at 14 (criticizing government efforts to filter Internet content); Editorial, *Net-*

as Save the Children).[39] Groups such as the Australian Christian Lobby, however, have been supportive.[40] Minority party senators, such as Steve Fielding of the Family First Party, have pressured the government to expand blocking.[41] Some stakeholders have supported filtering within limits, such as the child protection group Child Wise, which wants censorship limited to child pornography.[42] ISPs have had mixed reactions, evincing concerns both about acting as censors and about losing influence over filtering policy if they fail to engage the government.[43] Several major ISPs, though, have refused to participate in expanded trials of the filtering system.[44] The Australian Computer Society ("ACS") issued a mixed review of the proposal, cautioning that greater governmental specificity and data from multi-ISP trials are needed

Nanny State Worth Watching, AUSTRALIAN, Jan. 3, 2008, at 9 (discussing worrying aspects of the government's plan to filter Internet content); Computerworld, *supra* note 11 (voicing concerns over the government's proposed Internet filtering plan).

[38] *See, e.g.*, Paul Syvret, *Net Censorship Under Attack*, COURIER-MAIL, Jan. 19, 2008, at 56 (quoting the concerns of a librarian at the University of Technology in Sydney).

[39] *See* Asher Moses, *Children's Welfare Groups Slam Net Filters*, THE AGE (Melbourne), Dec. 1, 2008, http://www.theage.com.au/articles/2008/11/28/1227491813497.html?page=fullpage (quoting a member of Save the Children as saying that educating kids and parents was the way to empower young people to be safe internet users).

[40] *Australia to Implement Mandatory Internet Censorship*, HERALD SUN, Oct. 29, 2008, http://www.heraldsun.com.au/news/mandatory-censorship-on-web/story-0-1111117883306.

[41] *See* Nate Anderson, *Australia's Internet Filter: Could Legal Content Be Banned, Too?*, ARS TECHNICA, Oct. 28, 2008, http://arstechnica.com/news.ars/post/20081028-australias-internet-filter-could-legal-content-be-banned-too.html (last visited Nov. 12, 2009) (discussing Family First's role in influencing governmental Internet filtering); FAMILY FIRST, INTERNET PORNOGRAPHY AND CHILDREN 1 (2008), http://www.familyfirst.org.au/documents/INTERNETPORNOGRAPHYANDCHILDREN.pdf (advocating a "Mandatory Filtering Scheme at the ISP Server level").

[42] Fran Foo & Andrew Colley, *ISPs' Co-Operation Crucial to Federal Blocks on Child Pornography*, THE AUSTRALIAN, July 29, 2008, at 27 (quoting Child Wise chief executive Bernadette McMenamin).

[43] *Id. See also* Fran Foo, *Net Porn Filter Plan Needs Facelift*, AUSTRALIAN IT, Jan. 8, 2008, http://www.australianit.news.com.au/story/0,24897,23021650-16123,00.html (last visited Nov. 12, 2009) (noting opposition by Telstra BigPond, Australia's largest ISP).

[44] Asher Moses, *Labor Plan to Censor Internet in Shreds*, THE AGE, Dec. 9, 2008, *available at* http://www.theage.com.au/articles/2008/12/09/1228584820006.html.

before implementation.[45] The government has suggested that it may be flexible in its approach to filtering in some cases, such as with mobile phones, by requiring them to meet established standards while allowing the providers to use the technology of their choice.[46]

Recently, political prospects for legislation implementing filtering have worsened. Independent Senator Nick Xenophon, who initially indicated that he might support filtering (particularly if it included gambling sites), stated that he now opposes the plan as potentially counter-productive and a waste of funds.[47] Ironically, the communications spokesperson for the opposition Liberal Party, Nick Minchin, argues that legislation is required for mandatory filtering.[48] The opposition may be attempting to forestall governmental efforts to implement filtering through other means, such as public-private agreements similar to the one employed in the U.K.[49] While awaiting results from the large-scale trial of filtering in 2009, the Labor government appeared to retreat from its initial position on mandatory filtering, or at least to indicate greater flexibility. First, Minister Conroy stated that the mandatory blacklist of blocked sites would include only material classified Refused Classified ("RC"), rather than incorporating X – rated and 18-and-over ("R18") content.[50] Second, Conroy suggested filtering could take place through a voluntary ISP

[45] *See, e.g.*, Ben Grubb, *ACS Gives Conditional Thumbs Up to Internet Filtering*, IT NEWS AUSTRALIA., Oct. 12, 2009, http://www.itnews.com.au/News/158006,acs-gives-conditional-thumbs-up-to-internet-filtering.aspx (last visited Dec. 5, 2009) (reporting ACS support for filtering if five listed conditions are met by the federal government, including a specifically defined purpose of filtering).

[46] Andrew Colley, *Filtering standards to be eased for mobiles*, THE AUSTRALIAN, Sept. 30, 2008, at 30.

[47] Asher Moses, *Web censorship plan heads towards a dead end*, BRISBANE TIMES, Feb. 26, 2009, http://www.brisbanetimes.com.au/news/technology/web-censorship-plan-heads-towards-a-dead-end/2009/02/26/1235237821636.html (last visited Nov. 12, 2009).

[48] *Id.*

[49] *See generally* Frank Fisher, *Caught in the web*, THE GUARDIAN, Jan. 17, 2008, *available at* http://www.guardian.co.uk/commentisfree/2008/jan/17/caughtintheweb (discussing internet censorship by the Australian government).

[50] *Conroy clarifies Net filter plans*, WORLD NEWS AUSTL., Mar. 31, 2009, http://www.sbs.com.au/news/article/1013745/Conroy-clarifies-Net-filter-plans (last visited Nov. 12, 2009).

industry code to ban content, rather than through legislation.[51] ISPs already operate under voluntary codes addressing issues such as spam and online gambling, but it is not clear whether providers would voluntarily adopt content restrictions.[52] Australia's proposed Internet censorship produces a political conundrum: filtering was a key plank in Labor's electoral platform, but the government's efforts to implement (and expand) it have generated substantial opposition.

3. LEGAL CONTEXT

Australia regulates content through a classification system that divides material into prohibited, restricted, and generally available zones. Two specialized agencies, the ACMA and Classification Board, implement the statutory classification framework. This system has its oddities—the same material may be treated more harshly online than offline, and material hosted in Australia receives more careful review than content hosted abroad—but is generally familiar to and accepted by Australian citizens. However, the Labor government's proposal for generating block lists appears in tension with the complaint-based classification scheme used for Internet sites.

Australia's information regulation begins from an unusual point: the country's constitution contains no express guarantee of freedom of speech or expression[53] (though the High Court has found there is an implied right to political communication).[54]

[51] Andrew Colley, *Net Filtering May Not Be Mandatory*, AUSTRALIAN IT, May 26, 2009, http://www.australianit.news.com.au/story/0,27574,25542310-15306,00.html (last visited Nov. 12, 2009).

[52] *See* ACMA, Internet Codes Index, http://www.acma.gov.au/WEB/STANDARD/pc=IND_REG_CODES_INT (last visited Nov. 12, 2009) (provides access to a current list of "codes of practice" ISPs operate under based on legislation).

[53] *See* COMMONWEALTH OF AUSTRALIA CONSTITUTION ACT; Frederick Schauer, *On the Migration of Constitutional Ideas*, 37 CONN. L. REV. 907, 918 (2005) (noting that the Australian constitution does not contain a Bill of Rights). *See generally* EVAN CROEN, OPENNET INITIATIVE, AUSTRALIA AND NEW ZEALAND (May 15, 2007), http://opennet.net/research/regions/au-nz ("Without any explicit protection of free speech in the constitution, the Australian government has used its 'communications power' delineated in the constitution to regulate the availability of offensive content, endowing a government entity with the power to issue take-down notices for Internet content hosted within the country.").

[54] *See, e.g.*, Levy v. Victoria (1997) 189 C.L.R 579 (holding that the implied constitutional freedom of political speech is not absolute since laws that may

Information restrictions, or protections, thus derive primarily from the democratic political process rather than ex ante structural rules. This gives Australia's government greater leeway to censor Internet materials than would be possible in countries such as the United States, with its First Amendment, or Canada.[55] Filtering thus faces less judicial scrutiny, and Australia's constitution creates less need for the government to justify and tailor censorship than in other Western democracies.

Australia currently handles objectionable Internet content at the federal level via a complaint and takedown system under the Broadcasting Services Amendment (Online Services) Act of 1999.[56] The ACMA responds to complaints from Australian users,[57] and can initiate investigations on its own, by investigating whether Internet material qualifies as "prohibited content".[58] Prohibited content constitutes material that is classified[59] as X18 (non-violent, sexually explicit activity between consenting adults), R18 (likely to disturb or harm minors), RC (refused classification), and, in some cases, MA15+.[60] To categorize material hosted in Australia, the

restrict political communication are valid if they are meant to achieve a legitimate purpose).

[55] *See* Paula Baron, *The Moebius Strip: Private Right and Public Use in Copyright Law*, 70 ALB. L. REV. 1227, 1252 (2007) (discussing how "the lack of a free speech guarantee" can affect public access to information, such as the Internet).

[56] Broadcasting Services Amendment (Online Services) Act 1999, No. 90 (amending Broadcasting Services Act, No. 110 (1992) (Austl.)) (Austl.). *See generally* Christopher Stevenson, Note, *Breaching the Great Firewall: China's Internet Censorship and the Quest for Freedom of Expression in a Connected World*, 30 B.C. INT'L & COMP. L. REV. 531, 535 (2007) (discussing Australia's Internet censorship method of relying on reports by the public to identify prohibited online content and classify it).

[57] S*ee* Broadcasting Services Act, No. 110, §§ 147, 149 (1992) (Austl.); ACMA, Prohibited Online Content, http://www.acma.gov.au/WEB/STANDARD/pc=PC_90102 (last visited Nov. 8, 2009) (providing a checklist for filing a complaint, such as being an Australian resident, knowing the Internet address, and having reasons to believe the online content is prohibited).

[58] *See generally* ACMA, Online Regulation, http://www.acma.gov.au/WEB/STANDARD/pc=PC_90169 (last visited Nov. 8, 2009)

[59] *See* NATIONAL CLASSIFICATION CODE, FED. REG. OF LEGIS. INSTRUMENTS F2005L00816 (Austl.), *available at* http://www.comlaw.gov.au/ComLaw/Legislation/LegislativeInstrument1.nsf/0/B0644DBE6C7780F8CA256FD6001312BE/$file/National+Classification+Code+for+tabling+and+registratio.pdf (describing films, documentaries, and publications that are classified under each category).

[60] ACMA, *supra* note 57.

ACMA relies upon the Classification Board,[61] which applies the National Classification Code[62] and the Guidelines for the Classification of Films and Computer Games[63] developed under the Commonwealth Classification (Publications, Films, and Computer Games) Act of 1995.[64] Classification Board decisions can be appealed to the Classification Review Board.[65] If the material is hosted outside Australia, the ACMA estimates how the Classification Board would categorize the material, but does not submit the content to the Board.[66] Oddly, the classification scheme treats Internet material like films,[67] even if it is identical to content published in print offline, potentially leading to disparate treatment for the same information depending upon its medium.[68] More disturbingly, decisions by the Classification Board or the

[61] *See* Classification Board, The Classification Website, http://www.classification.gov.au/www/cob/classification.nsf/Page/Classification_in_AustraliaWho_we_areClassification_Board (last visited Nov. 8, 2009); The Classification Website, Classification Review Board, http://www.classification.gov.au/www/cob/classification.nsf/Page/Classification_in_AustraliaWho_we_areReview_Board (last visited Nov. 8, 2009).

[62] *See supra* note 59 and accompanying text.

[63] Guidelines for the Classification of Films and Computer Games, FED. REG. OF LEGIS. INSTRUMENTS F2008C00126 (Austl.), *available at* http://www.comlaw.gov.au/ComLaw/Legislation/LegislativeInstrumentCompilation1.nsf/0/F0EC030A108C93DDCA2574120004F6B8/$file/FCGGuidelines2005.pdf (explaining the criteria for classifying publications and films under the 1995 amendment in user-friendly language).

[64] Classification (Publications, Films and Computer Games) Act, 1995, No. 7 (1995) (Austl.) (setting out the requirements for the application and review of classifying media content).

[65] The Classification Review Board, http://www.classification.gov.au/www/cob/classification.nsf/Page/ClassificationinAustralia_Whoweare_ReviewBoard_ReviewBoard (last visited Oct. 26, 2009)

[66] ACMA, What Will ACMA Do?, http://www.acma.gov.au/WEB/STANDARD/pc=PC_310147#whatwill (last visited Dec. 4, 2009) (describing the steps ACMA will take if content is prohibited or not hosted in Australia).

[67] *See* Classification (Publications, Films, and Computer Games) Act 1995 § 5 (defining "film" to include "any other form of recording from which a visual image, including a computer generated image, can be produced").

[68] *See* Australian Government, Attorney-General's Department, Classification Categories and Markings, http://www.ag.gov.au/www/agd/agd.nsf/Page/Classificationpolicy_Classificationcategoriesandmarkings (last visited Oct. 26, 2009) (comparing classification schemes for films, Internet material and publications).

ACMA on Internet material are secret, unlike decisions on offline content.[69]

If the Classification Board finds that the website constitutes prohibited content, the ACMA sends a takedown notice to the ISP or Internet Content Host.[70] If the ACMA believes material constitutes prohibited content, or *may* constitute prohibited content, but is not hosted in Australia, the ACMA notifies Web blocking software vendors to add the site to their block lists.[71] The ACMA maintains a "black list" of roughly 1100 sites that should be blocked by these vendors.[72] While the Rudd government has implied that these sites are almost entirely composed of child pornography, approximately 49% of the list's sites were child pornography, 63% were RC content, and 32% were X18+ material.[73] One site on the black list, for example, is an anti-abortion website, whose pictures of aborted fetuses led to its categorization as RC.[74] An ACMA spokesperson, testifying before a parliamentary committee, stated that the Authority would seek to block content classified as RC, X18+, or R18+ that is not protected by an age verification system.[75] ACMA's blacklist thus includes material, such as R18+ content, that is lawful for adults to view and possess.

This legal mechanism has been employed to generate, through the combination of complaints, investigations, and classification, the blacklist of sites compiled by the ACMA. Whether ISPs will be required to block only these sites, or must also filter additional material, is both unclear and contested. Political representatives

[69] Electronic Frontiers Australia, FOI Request on ABA, http://www.efa.org.au/FOI/foi_aba_2000.htm (last visited Oct. 26, 2009) (discussing the Administrative Appeals Tribunal decision to black out URLs on documents before releasing them to Electronic Frontiers Australia).

[70] ACMA, Regulating Online Content, http://www.acma.gov.au/WEB/STANDARD/pc=INT_IND_CONTENT_ABOUT (last visited Dec. 4, 2009).

[71] *Id.* (stating that ACMA will notify suppliers of approved filters if the content is not hosted in Australia, but is likely prohibited).

[72] Fran Foo, *Row Over Web blacklist*, AUSTRALIAN IT, Feb. 24, 2009, http://www.australianit.news.com.au/story/0,24897,25096792-15318,00.html (quoting ACMA figure of 1090 sites as of January 31, 2009).

[73] *Id.* (quoting November 30, 2008 figures which involved 1370 pages, including 864 RC content links, 674 child pornography links, and 441 X18+ links). The total exceeds 100% as a site may be both child pornography and RC.

[74] *Id.*

[75] John Ozimek, *Aussie Internet-Net Will Be Drawn Wider*, THE REGISTER, Feb. 25, 2009, http://www.theregister.co.uk/2009/02/25/oz_internet_net/.

such as Senator Fielding have argued for expanding filtering to additional classification categories such as R18+,[76] though the government has shifted its stance on what material should be placed on the mandatory blacklist.[77]

Australia's states and territories also have an admixture of Internet content regulatory laws. Some have laws stricter than the federal scheme (such as Victoria), some have information-restricting laws that do not cover online material (such as Tasmania), and some have regulations that are more stringent in some respects and more lax in others compared to federal law (such as Western Australia).[78]

An additional issue that may be legally problematic is Labor's proposal to incorporate lists of child pornography from other sources—particularly Britain's Internet Watch Foundation ("IWF")[79]—into the list of sites that must be blocked[80]. This idea generates two problems. First, it flies in the face of the complaint-based model used to determine what Internet content is prohibited.[81] Incorporating other block lists into filtering effectively shifts, or outsources, responsibility for classification from the ACMA and the Classification Board to foreign third parties with no responsibility to, or accountability in, Australia. While the ACMA might treat foreign block lists as complaints and vet the sites on them for illegality, this practice may contravene

[76] Nate Anderson, *Australia's Internet Filter: Could Legal Content Be Banned, Too?*, ARS TECHNICA, Oct. 28, 2008, http://arstechnica.com/news.ars/post/20081028-australias-internet-filter-could-legal-content-be-banned-too.html.

[77] *See, e.g.,* Asher Moses, *Christians Upset at Conroy's Net Policy "Backtrack,"* SYDNEY MORNING HERALD, May 27, 2009, *available at* http://www.smh.com.au/news/technology/web/christians-upset-at-conroys-net-policy-backtrack/2009/05/27/1243103585180.html (discussing the debate around whether the government should soften its policy to censor Internet content).

[78] *See* Electronic Frontiers Australia, *Internet Censorship Laws in Australia* (Mar. 31, 2006), http://www.efa.org.au/Issues/Censor/cens1.html#sandt (outlining the different types of legislation enacted by States and Territories that enable prosecution of Internet users that make available or download child pornography).

[79] Internet Watch Foundation, http://www.iwf.org.uk (last visited Dec. 11, 2008)

[80] Moses, *supra* note 44.

[81] The ACMA has begun researching this issue. *Testimony of Nerida O'Loughlin before the Standing Committee on Environment, Communication, and the Arts* 65–66 (2009), *available at* http://www.aph.gov.au/hansard/senate/committee/S11635.pdf.

Australian law by treating foreign complainants as equal with Australian ones.[82]

Second, while child pornography might seem amenable to a universal definition, this is not empirically true. Graphic sexual cartoons of Bart and Lisa Simpson (from the television program "The Simpsons") likely would not qualify as child pornography in the United States,[83] but might in Australia.[84] Similarly, both Australia and the U.S. ban the possession of nude images of 16-year-olds, but Japan does not.[85] The IWF classified the cover of a music album from 1976 (which featured a picture of a nude girl) as child pornography, and then reversed itself.[86] Including foreign lists of child pornography into Australia's block list undercuts the country's ability to render its own, sovereign judgments about what material is unlawful and transfers authority for such decisions to unaccountable third parties who may use different standards.

Overall, Australia's scheme for classifying Internet content — in particular its federal system with the Classification Board and the ACMA—sets out the legal backdrop for decisions on what material to filter. While Australia's system for content ratings and restrictions is well-established, its application to the Internet in the context of filtering is proving controversial.

[82] *See generally* AMCA, *supra* note 57 (requiring that a complainant be an Australian or a company based in Australia).

[83] Ashcroft v. Free Speech Coal., 535 U.S. 234 (2002) (ruling that virtual child pornography is protected under the First Amendment). *But see* United States v. Whorley, 550 F.3d 326 (4th Cir. 2008) (upholding a conviction for the violation of a statute prohibiting the act of knowingly receiving obscene material).

[84] McEwen v. Simmons & Anor (2008) N.S.W.S. Ct. R. 1292; *see generally* Bellinda Kontominas, *Simpsons Cartoon Rip-off is Child Corn—Judge*, SYDNEY MORNING HERALD, Dec. 8. 2008, *available at* http://www.stuff.co.nz/4786351a1860.html (explaining the ruling of an Australian Supreme Court judge who ruled that an Internet cartoon in which characters from *The Simpsons* engage in sexual acts is child pornography).

[85] *See* Jake Adelstein, *This Mob Is Big in Japan*, WASH. POST, May 11, 2008, at B2 (noting Japan does not criminalize possession of child pornography, though it does ban distribution and production).

[86] *IWF Backs Down on Wiki Censorship,* BBC NEWS, Dec. 9, 2008, *available at* http://news.bbc.co.uk/2/hi/technology/7774102.stm. The offending image is available from Wikipedia, *Virgin Killer*, *at* http://en.wikipedia.org/wiki/Virgin_Killer.

4. TECHNOLOGICAL CONTEXT

Australia is trying to adapt filtering practices to its decentralized network architecture. To refine implementation, the Labor government launched an initial pilot on one ISP, and is beginning a larger-scale trial. The proposed system has two levels: a mandatory block of at least the ACMA block list and an "opt-out" layer that filters material inappropriate for children but permissible for adults.[87] Initial testing shows that filtering faces several challenges. First, the government has been ambiguous about the scope of targeted content. Second, blocking inevitably restricts both too much and too little content, even when there is consensus on what should be filtered. Finally, there is a collateral cost to filtering: adverse performance effects and reduced Internet access speeds. The "tax" in access speed and added cost that filtering imposes creates tension between Australia's efforts to censor the Internet and its goal of expanding broadband access.[88]

From a technological perspective, Australia offers a fascinating test case: the country seeks to retrofit Internet filtering to a network infrastructure that did not contemplate this need as a design goal.[89] Authoritarian countries have often built their network infrastructures with information control as an express requirement: Saudi Arabia created an architecture where Internet traffic flows through three "choke points" overseen by the Communications and Internet Technology Commission, allowing filtering to occur at three centralized locations.[90] Similarly, China deployed its networks to allow censorship to occur at multiple control points, from international gateways to the network backbone to regional network providers.[91]

[87] *See, e.g.,* Foo, *supra* note 14 (reporting the timeline for ISP filtering trials).

[88] *See* AUSTRALIAN COMPUTER SOCIETY, TECHNICAL OBSERVATIONS ON ISP BASED FILTERING OF THE INTERNET 3, 12–15 (Oct. 2009), https://www.acs.org.au/attachments/2009/ispfilteringoct09.pdf (describing the complexity inherent in the development of Australia's Internet filtering system).

[89] *See* Croen, *supra* note 533 (providing an overview of both the Australian and New Zealand approach to filtering Internet content).

[90] *See* Content Filtering in Saudi Arabia, http://www.internet.gov.sa/learn-the-web/guides/content-filtering-in-saudi-arabia (last visited Dec. 6, 2009).

[91] *See* ETHAN GUTMANN, LOSING THE NEW CHINA: A STORY OF AMERICAN COMMERCE, DESIRE, AND BETRAYAL 127–32 (2004) (explaining Chinese motivation for and approach to control over Internet architecture); JONATHAN L. ZITTRAIN & JOHN G. PALFREY, JR., INTERNET FILTERING IN CHINA IN 2004–2005: A COUNTRY STUDY 48–49 (Apr. 2005), http://opennet.net/sites/opennet.net/files/ONI_China

Australia's Internet deployment, in contrast, was driven by user demand for access to the Web and emerged in a more free-form, market driven fashion, rather than following a centralized plan or model.[92] Thus, Australia lacks a single nexus—or even a small number of network nodes—where filtering can be deployed to achieve complete coverage. ISPs must necessarily be involved in censorship if it is to be mandatory and universal. (How this distributed model compares to centralized filtering in terms of performance and effects on network speeds is not certain; filtering could be faster if its workload were distributed by being placed closer to the network edge or faster if placed closer to the core where it could achieve efficiencies of scale and avoid redundancy.) [93] It can also increase the challenge of keeping block lists up to date; as there are more network points where the lists are implemented, it becomes more challenging to ensure each list is properly updated. The outcome of Australia's experiment with applying mandatory filtering in the decentralized environment of a Western democratic nation will have much to teach other countries considering similar systems.

The current Labor filtering plan contemplates a two-tiered system. The first level would block access to ACMA's blacklist. This filter would be mandatory for all users. The second level would block material categorized as inappropriate for children, such as pornography and violence, and could be bypassed by users on request (an opt-out system).[94] The government has not specified clearly what types of material would be censored by either tier of filtering, though it appears to have moved towards mandating the blocking of only RC material.[95]

_Country_Study.pdf (reporting research results that reflect China's multi-tiered approach to control of information online).

[92] *See* Roger Clarke's Website, Origins and Nature of the Internet in Australia: The Beginnings of the Australian Internet, http://www.rogerclarke.com/II/oz104.htmlo#beg (last visited Oct. 27, 2009) (mapping the rise of the Australian Internet connectivity from a university-centered system to a national network).

[93] *See* AUSTRALIAN COMPUTER SOCIETY, *supra* note 88, at 12 (outlining the numerous considerations presented by the decision of where to filter within an ISP network).

[94] *See, e.g.,* Nick Bryant, *Australia Trials National Net Filters*, BBC NEWS, Oct. 25, 2008, http://news.bbc.co.uk/2/hi/technology/7689964.stm (presenting Australian politician Stephen Conroy's explanation of the filtering project in contrast with the popular reaction that it has provoked).

[95] *See* AUSTRALIAN COMPUTER SOCIETY, *supra* note 88, at 3 ("[R]ecent Government statements indicate that ISP level filtering will apply to RC material

No filtering system is impermeable, however. Technologically-adept users have already begun to test—and share—methods to circumvent filtering once it is implemented. The range of circumvention methods is broad,[96] and includes tactics such as requesting Web pages through a proxy server,[97] using encryption, and employing alternative network paths through services such as Tor, also known as "the onion router," which enhances Internet privacy by bypassing traffic analysis.[98] While the government optimistically regards the risk of circumvention as low,[99] technically skilled users have long bypassed filtering in sophisticated systems such as those of China[100] and Iran.[101]

that is on the ACMA blacklist, [but] there is still a considerable amount of confusion amongst the ICT sector on exactly what content will be filtered.").

[96] *See generally* Nart Villeneuve, *Choosing Circumvention: Technical Ways To Get Round Censorship, in* REPORTERS WITHOUT BORDERS, HANDBOOK FOR BLOGGERS AND CYBER-DISSIDENTS 63 (2005), http://www.rsf.org/IMG/pdf/handbook_bloggers_cyberdissidents-GB.pdf (providing insight into the various forms of "circumvention technologies" that allow people to avoid online censorship and surveillance efforts).

[97] *See, e.g.,* Contempt by Paul Dwerryhouse, How to Bypass Australia's Forthcoming Internet Filter, http://weblog.leapster.org/archives/122-How-to-bypass-Australias-forthcoming-internet-filter.html (Nov. 13, 2008, 18:17) (describing use of SSH as a SOCKS proxy to a remote server).

[98] *See* Tor: Overview, http://www.torproject.org/overview.html.en (last modified March 3, 2009) (explaining how the system enhances privacy by keeping users anonymous through distribution of transaction points, and also giving examples of how people use the system to access Internet services and communicate with others).

[99] AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY, *supra* note 8, at 9 (assessing the relative levels of probability that various forms of Internet filtration will be circumvented).

[100] *See, e.g.,* Sumner Lemon, *Group Offers Tools to Evade China's Web Censorship*, PC WORLD, Aug. 4, 2008, http://www.pcworld.com/businesscenter/article/149341/group_offers_tools_to_evade_chinas_web_censorship.html (reporting on the availability of software that allows reporters in China to circumvent online government filters).

[101] *See, e.g.,* THE CITIZEN LAB, University of Toronto, EVERYONE'S GUIDE TO BY-PASSING INTERNET CENSORSHIP 16 (Sept. 2007), http://citizenlab.org/CL-circGuide-online.pdf (offering one example of an activist "tunneling" past Chinese Internet firewalls in order to post otherwise censored information); Nart Villeneuve, *Evasion Tactics*, 36 INDEX ON CENSORSHIP 71, 75 (Nov. 2007), *available at* http://www.nartv.org/mirror/evasiontactics-indexoncensorship.pdf (referencing a widespread Iranian practice of dodging Internet filters in order to follow the writings of bloggers).

To evaluate potential filtering methods and to answer critics, the Rudd government launched a first-stage pilot program.[102] The trial evaluated six filtering products in effects on network performance, effectiveness in blocking access to prohibited sites, and inadvertent blocking of permitted sites. The trial, run by Enex TestLab, took place on the network of the ISP Telstra in Tasmania.[103] Telstra did not participate in the test's implementation other than by providing network access, and had no specific knowledge of its methodology or results.[104]

The pilot evaluated the products' effectiveness by testing three lists of URLs that were vetted by the ACMA.[105] The first list (Category 1) contained 1000 URLs categorized as prohibited content. The second list (Category 2) contained 933 URLs that, while not illegal, might be inappropriate for minors. The third list (Category 3) contained 1997 URLs that were permissible for minors. The trial evaluated under-breadth—failure to block prohibited material—by measuring the percentage of sites in Categories 1 and 2 that a product filtered.[106] (Here, a perfect score would be 0%.)[107] It measured over-breadth—filtering of sites without illicit content—by measuring the percentage of sites in Category 3 that a product blocked.[108] (Perfection would be 0%.) Results varied greatly: under-breadth ranged from a low of 2% to a high of 13% across the six products; over-breadth ranged from a low of 1.3% to a high of 7.8%.[109] Filtering products that blocked more banned sites also tended to block more innocent ones.[110]

[102] *See generally* Liam Tung, *BitTorrent hole in ISP filter tests*, ZDNET AUSTL., July 18, 2008, http://www.zdnet.com.au/news/communications/soa/BitTorrent-hole-in-ISP-filter-tests/0,130061791,339290888,00.htm (reporting on the federal government's release of the results of ISP-level content filtering tests).

[103] AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY, *supra* note 8, at 17–18, 22.

[104] *Id.*

[105] *Id.* at 20–22.

[106] *Id.* at 35, 37.

[107] Zero under-breadth would mean that the difference between the total sites tested in Categories 1 and 2 and the total sites blocked divided by the total sites tested in Categories 1 and 2 equals zero.

[108] AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY, *supra* note 8, at 35, 37.

[109] *Id.* at 62–68.

[110] *See* discussion of these results *infra* Section 5.2.

The test also demonstrated that all but one product had a significant, detrimental effect on network performance (the amount of data per unit time that the network could transport). Enex TestLab measured three data points (all calculated as the number of transactions per second the network could support): a baseline; the decrease in performance when the filtering product was installed but not blocking content ("passive"); and the decrease in performance when the filtering product blocked material ("active").[111]

As with effectiveness, performance impact varied. Of the six tested products, five reduced performance in passive mode by 8% or less (one incurred a performance hit of 22%).[112] When switched into active mode, though, five products reduced performance by 20% or more (one maintained 98% performance).[113] The worst product throttled network speed to 16% of the baseline measure.[114] ISPs may incur significant performance penalties when filtering, though the effect depends greatly upon the product that they use. Minister Conroy has dismissed performance concerns, noting that the "internet hasn't ground to a halt in the UK, [and] it hasn't ground to a halt in Scandinavian countries."[115]

Filtering Product	**Passive Performance (baseline = 100)**	**Active Performance (baseline = 100)**
Alpha	92	16
Beta	99	67
Gamma	98	14
Delta	99	98
Theta	78	76
Omega	101	79

[111] AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY, *supra* note 8, at 34.

[112] *Id.* at 62–68.

[113] *Id.*

[114] *Id.* at 60 (describing the filtering product Alpha).

[115] *Conroy Announces Mandatory Internet Filters to Protect Children*, AUSTL. BROAD. CORP. NEWS, Dec. 31, 2007, http://www.abc.net.au/news/stories/2007/12/31/2129471.htm [hereinafter *Mandatory Internet Filters*]

TABLE 1 - PERFORMANCE EFFECTS IN FILTERING TRIAL[116]

In late 2008, the government released technical specifications for a second, broader filtering trial.[117] The second pilot invited ISPs at all industry levels to participate—though a number of prominent providers have refused[118]—and to select from a range of filtering options, from blocking only the ACMA's blacklist to more broadly targeting sensitive content.[119] ISPs were encouraged to enroll customers voluntarily in the trial.[120] Testing will be conducted for a range of network bandwidths (from 56 Kbps to 12 Mbps) and physical media;[121] commentators have criticized the limited bandwidth as likely to distort results.[122]

The second test expands upon the initial Tasmanian pilot in several key respects. It includes more ISPs,[123] envisions blocking an ACMA-mandated list of up to 10,000 URLs (including lists of child pornography from other sources, such as Britain's Internet Watch Foundation),[124] and tests different technical variants of

[116] AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY, *supra* note 8, app. f at 62–68.

[117] DEP'T OF BROADBAND, COMMC'NS AND THE DIGITAL ECON., INTERNET SERVICE PROVIDER CONTENT FILTERING PILOT: TECHNICAL TESTING FRAMEWORK 1 (2008), *available at* http://www.dbcde.gov.au/__data/assets/pdf_file/0006/89160/technical-testing-framework.pdf

[118] *See, e.g.*, Fran Foo, *Telstra says no to filtering trials*, AUSTL. IT, Dec. 9, 2008, http://www.australianit.news.com.au/story/0,24897,24771009-15306,00.html (reporting that Telstra and Internode, two of Australia's largest ISPs, both declined to participate in content filtering trials).

[119] DEP'T OF BROADBAND, COMMC'NS AND THE DIGITAL ECON., *supra* note 117, at 2; Moses, *supra* note 44; *see also* Foo, *supra* note 14 (noting TECH 2U will let participating customers designate additional content categories for blocking).

[120] Foo, *supra* note 14.

[121] DEP'T OF BROADBAND, COMMC'NS AND THE DIGITAL ECON., *supra* note 117, at 8.

[122] *See, e.g.*, Darren Pauli, *Optus, iiNet Put Filters to the Test*, COMPUTERWORLD, Nov. 13, 2008, http://www.computerworld.com.au/article/267223/optus_iinet_put_filters_test (reporting that trials restricted to 12 Mbps will undermine final test results since they are only a "small fraction of ISP network connections").

[123] The government received applications from sixteen ISPs and initially selected six. Foo, *supra* note 14. Some ISPs, such as iiNet, sought to participate to demonstrate "how stupid it is." Asher Moses, *Net censorship plan backlash*, THE AGE (Melbourne), Nov. 11, 2008, http://www.theage.com.au/news/technology/biztech/net-censorship-plan-backlash/2008/11/11/1226318639085.html?page=fullpage#contentSwap1 (quoting iiNet managing director Michael Malone who was participating in the trials to give hard data that the system would not work).

[124] DEP'T OF BROADBAND, COMMC'NS AND THE DIGITAL ECON., *supra* note 117, at 4; Moses, *supra* note 44. *But see IWF backs down on Wiki censorship*, *supra* note 86

filtering (such as blocking IP addresses versus URLs, or altering Domain Name Service results).[125] The test also considers additional variables that will affect implementing filtering, such as ease of circumventing blocking, cost, ease of use, effectiveness at blocking non-Web content, and scalability.[126] Interestingly, the trial's framework contemplates using a user complaint system not only to determine sites to block (which the ACMA already does), but also to reduce over-blocking by identifying sites that are inadvertently filtered.[127] This next phase of testing provides further data to guide implementation of the Labor government's filtering program.

The Tasmanian (first) trial run of filtering has not assuaged critics of the government's plan, and demonstrates that censorship incurs information costs as well as financial and technological ones. The information costs are threefold. First, users will inevitably be unable to access permitted sites due to inadvertent over-blocking.[128] Second, either their connection speed will slow due to the network latency introduced by filtering, or users will have to pay more for the same speed of Internet access. Third, filtering cannot now prevent access to much illicit content online. Currently, most filtering products offer only crude, all-or-nothing capabilities for content communicated over e-mail, peer-to-peer file sharing, instant messaging, and other protocols, either blocking them completely or letting their traffic pass unfettered. The filtering programs tested by Australia all censor Web-based material ("HTTP"), but only five claim to block secure Web traffic ("HTTPS"), two claim to filter e-mail content, and one claims to filter streaming video.[129] This means that filtering can prevent casual or easy access to banned material, but is less successful in

(reporting Internet Watch Foundation's withdrawal of its objection to a Wikipedia page containing suspected child pornography).

[125] DEP'T OF BROADBAND, COMMC'NS AND THE DIGITAL ECON., *supra* note 117, at 3.

[126] *Id.*

[127] *Id.* at 5.

[128] *Cf.* INTERNET FILTERING IN SAUDI ARABIA IN 2004, http://opennet.net/studies/saudi#toc1d (last visited Dec. 3, 2009) (describing inadvertent blocking in Saudi Arabia due to classification errors).

[129] AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY, *supra* note 8, at 44–45.

disrupting determined attempts to share it.[130] Child pornography, for example, is increasingly shared over peer-to-peer networks rather than the Web.[131] This implies that filtering can reduce access to child pornography, and similar unlawful material, but cannot eliminate it.[132] These costs are real and must be weighed against the benefits filtering achieves.

Moreover, these challenges create implicit tensions in Australia's larger Internet policy agenda. If the pilot filtering program results are accurate, implementing censorship will reduce Internet access speeds—perhaps significantly. This could undercut Australia's efforts to drive broadband deployment.[133] Filtering could effectively reduce broadband to lower-bandwidth access. For example, the Organization for Economic Co-operation and Development defines "broadband" as having a minimum access speed of 256 kilobits per second ("kbps").[134] A 20% reduction in speed would drop such a connection to 205 kbps, and a 75% reduction would drop it to 64 kbps—barely faster than dial-up access.[135] Filtering acts as a tax: customers not only pay censorship costs directly (through levies passed on by ISPs), but indirectly, as ISPs will need to account and charge for, the bandwidth overhead of filtering when offering access at various speeds. Similarly, ISPs

[130] *See generally* AUSTL. COMPUTER SOC'Y, *supra* note 88, at 5 (exploring the best approaches to ISP filtering while recognizing there are many ways to circumvent these efforts).

[131] *See generally Stumbling onto Smut: The Alarming Ease of Access to Pornography on Peer-to-Peer Networks: Hearing Before the H. Comm. on Gov't Reform*, 108th Cong. 27–48 (2003) (statement of Linda D. Koontz, Director, Information Management Issues, U.S. General Accounting Office) (providing data that child pornography is easily found and downloaded from peer-to-peer networks); Press Release, Dep't of Justice, Multi-Agency Investigation Targets Use of Peer-to-Peer Networks to Exchange Child Pornography (Aug. 19, 2008), *available at* http://losangeles.fbi.gov/dojpressrel/pressrel08/la081908usa.htm (discussing a multiple-agency effort to target those using peer-to-peer networks to exchange child pornography).

[132] *See* Moses, *supra* note 39 (quoting David Vale, Executive Director of UNSW's Cyberspace Law and Policy Centre as saying, "[t]here seemed to be some consensus that the proposed mandatory filter model would not actually be directed at the real channel of child porn distribution, which is not the blacklist of known web sites, but via various other internet protocols and tools").

[133] AUSTRALIAN LABOR PARTY, *supra* note 9, at 23–24.

[134] ORG. FOR ECON. CO-OPERATION AND DEV., OECD BROADBAND SUBSCRIBER CRITERIA (2008), http://www.oecd.org/document/46/0,3343,en_2649_34225_39575598_1_1_1_1,00.html.

[135] Five of six products tested in the initial trial caused at least 20% decreases; two caused at least 75% drops.

will need to invest in additional network capacity, incurring costs. The ACMA estimates that a provider with a four-year upgrade cycle for its networking equipment would, when faced with a 25% performance decrease from filtering, be forced to move to a three-year upgrade cycle. Censorship's cost—the filtering tax—is thus both technical (access speed) and financial (increased overhead and cost of equivalent access).

Technologically, the Rudd government seeks to mandate that ISPs retrofit filtering to a heterogeneous network architecture designed to avoid network blockages of exactly the type that online censorship creates. The cost, difficulty, and performance drop that the country's Internet access suffers as a result of filtering will guide other nations that consider implementing broad, mandatory content restrictions online.

5. ANALYSIS

Internet censorship used to be limited to bad actors: authoritarian regimes such as China and Iran, or non-democratic countries with limited protections for civil liberties such as Saudi Arabia. A country's system of governance and protection for human rights could be used as a proxy for whether its online content restrictions were legitimate. This simple analytical rule no longer works—Britain,[136] Canada,[137] France,[138] Thailand,[139] India,[140]

[136] *See generally* Fisher, *supra* note 4.

[137] *See* CYBERTIP!CA, CLEANFEED CANADA, http://cybertip.ca/app/en/cleanfeed (last visited Dec. 4, 2009) (stating Canada's Cleanfeed system "aims to reduce accidental access to child sexual abuse images as well as to discourage those trying to access or distribute child pornography").

[138] *See France Blocks Online Child Porn, Terrorism, Racism*, U.S.A. TODAY, June 10, 2008, *available at* http://www.usatoday.com/tech/world/2008-06-10-france-online-porn_N.htm; Declan McCullagh, *Google Excluding Controversial Sites*, CNET NEWS.COM, Oct. 23, 2002, http://www.news.com/2100-1023-963132.html (stating that Google has deleted controversial sites in France); SANGAMITRA RAMACHANDER, OPENNET INITIATIVE, EUROPE, http://opennet.net/research/regions/europe (last visited Dec. 4, 2009) (discussing suits brought against Google and Yahoo by French entities).

[139] *See* Posting of C.J. Hinke to Global Voices Advocacy, Censoring Free Speech in Thailand (May 17, 2008), http://advocacy.globalvoicesonline.org/2008/05/17/censoring-free-speech-in-thailand.

[140] *See* OPENNET INITIATIVE, INDIA (2007), http://opennet.net/research/profiles/india (stating that the Department of Telecommunications announced that mechanisms would be installed to filter websites in India).

and Turkey[141] all filter the Internet within a democratic framework.[142] Thus, we need a more sophisticated way to judge whether Internet censorship is legitimate.

In a recent article, I describe a new four-part methodology to assess the legitimacy of a country's Internet filtering.[143] The methodology employs a process-based approach to enable normative analysis that is separate from an observer's perspective on which content may legitimately be targeted for censorship. In other words, it seeks to enable you to assess whether a country's blocking of pornography is legitimate regardless of whether you approve of filtering porn. Briefly, the four-part framework evaluates a country's filtering based on whether it is open (does the nation admit that it censors, and why?), transparent (does the country describe the material that it blocks and its criteria for classification?), narrow (does the filtering block proscribed material effectively and leave lawful material untouched?), and accountable (does the country respond to users' desires regarding filtering, and are decisionmakers subject to challenge for erroneous choices?). Legitimate filtering is open, transparent, narrowly focused, and accountable to citizens. The paper proposes that different analysts and stakeholders should develop quantitative metrics to measure countries upon these four axes, with the resulting competition among the metrics driving refinement and improvement. Since this iterative process has not yet taken place, the next section offers a preliminary assessment of Australia's proposed filtering system based on these four criteria.

5.1. Openness

Australia is quite open about its filtering intentions. The Labor Party included a proposal to censor Internet content in its official National Platform for the most recent federal election.[144] Minister

[141] *See* Jeffrey Rosen, *Google's Gatekeepers*, N.Y. TIMES MAG., Nov. 30, 2008, at 50 (stating that "a Turkish judge had ordered the nation's telecom providers to block access to the [YouTube] site in response to videos that insulted the founder of modern Turkey"); Yigal Schleifer, *Turkey Tightens Controls on Internet Speech*, CHRISTIAN SCIENCE MONITOR, Oct. 30, 2008, *available at* http://www.csmonitor.com/2008/1030/p06s01-wome.html (discussing Turkey's ban on 850 websites).

[142] *See generally* ACCESS DENIED, *supra* note 1.

[143] Bambauer, *supra* note 16, at 390–410.

[144] AUSTRALIAN LABOR PARTY, *supra* note9.

Conroy has given press statements,[145] responded to questions in Parliament,[146] and put forth position papers outlining the government's intentions.[147] While Labor's cyber-safety plan emerged late in the electoral campaign, its content was similar to its earlier program from March 2006. The controversy over the filtering plan emerged precisely because of the Labor government's forthrightness on the subject.

The government has also been open about its normative reasons for engaging in filtering. The Labor Party's cyber-safety plan focuses on potential threats to children, such as exposure to "harmful and inappropriate online material," Internet sex predators and sex offenders, identity theft, and computer viruses.[148] The rationale for restricting other types of content—particularly that which would be lawful for Australians to view online normally or to access in offline media—is less clear, but builds upon the values and choices underlying the country's overarching content regulation scheme. This latter point is challenging to assess because the Labor government has not yet described what content, beyond that which is illegal, would be filtered, particularly by the opt-out layer of the system.

However, if the government does move to include material beyond the ACMA blacklist, it should be clear about why it targets that material. One rationale might be that the opt-out method for adults to view such sites functions as an effective age restriction on content similar to those used for movies.[149] This should create

[145] *See, e.g., Mandatory Internet Filters*, *supra* note 115.

[146] *Official Committee Hansard: Testimony Before the Sen. Standing Comm. on Env't., Commc'ns., and the Arts* 71-79 (2009) (Austl.) (statement of Sen. Stephen Conroy, Minister for Broadband, Communications and the Digital Economy), http://www.aph.gov.au/hansard/senate/commttee/S11635.pdf [hereinafter *Conroy Statement*]

[147] CONROY, *supra* note 6.

[148] CONROY, *supra* note 6, at 2–7.

[149] *Compare* CLASSIFICATION BOARD, COMPLIANCE FOR CINEMAS AND OTHER PUBLIC EXHIBITORS, http://www.classification.gov.au/www/cob/classification.nsf/Page/Industry_HowtoComplywithClassificationLaws_ComplianceforCinemasandOtherPublicExhibitors (last visited Dec. 4, 2009) (providing a guideline of compliance requirements), *with* ACMA, *Minimum Verification System Requirements: Restricted Access Systems Declaration 1999* (source on file with U. PA. J. INT'L. L) (setting out the minimum system requirements for a "restricted access system"), *and* Gerard Goggin, *Regulating Mobile Content: Convergences and Citizenship*, 12 INT'L J. COMM. L. & POL'Y 140, 149–52 (2008) (discussing mobile device content regulation).

added pressure, though, for the country to justify the disparate treatment of material online and offline.

Overall, Australia is open about its filtering, and scores highly for this criterion.

5.2. Transparency

To date, Australia's transparency regarding its filtering has been poor. The country has vacillated on what material it will target for blocking.[150] This uncertainty makes it difficult for citizens to assess whether the scope of material blocked is appropriate, and whether the set of targeted sites comports with the underlying rationales for censorship. The Labor government is opaque about the types of sites that will be blocked, how a site will be evaluated for filtering, and how those decisions map to larger social and political goals.

Transparency measures how clearly the government discloses what content it seeks to block and explains why that material runs counter to its goals. By being transparent, a country lets citizens assess how the banned sites relate to the government's broader rationales for censorship. A country filtering the Internet to prevent harm to children could target pornography, extreme violence, or illegal drugs sites—or all three. Transparency varies along a continuum, from disclosing the list of sites blocked (which Australia has refused to do) to describing vague guidelines for prohibited content. A key feature of transparency is that it can be tested: groups such as Reporters Without Borders[151] and the OpenNet Initiative[152] can challenge a government's claims by checking what sites are blocked. If the country claims only to block material harmful to youth, but censors the political opposition while failing to filter pornography, it is plainly not being transparent.[153]

[150] *See Conroy Statement*, *supra* note 146 (indicating much recent debate in Australia on the issue).

[151] *See, e.g.*, REPORTERS WITHOUT BOREDERS: TUNISIA, http://www.rsf.org/article.php3?id_article=26158&Valider=OK (last visited Dec. 4, 2009) (providing an example of how Reporters Without Borders challenges governmental claims).

[152] *See generally* ACCESS DENIED, *supra* note 1 (explaining how the OpenNet Initiative challenges governmental claims).

[153] Vietnam, for example, claims to censor only pornography. However, the country blocks zero pornographic sites, but does block a host of political ones. *See* OPENNET INITIATIVE: VIETNAM, May 9, 2007, http://opennet.net/research/profiles/vietnam.

It is clear that the system will filter at least some illegal material, such as child pornography.[154] The blacklist of sites compiled by the ACMA is sure to be blocked. However, recently Minister Conroy outlined a plan to expand blocking to include "other unwanted content," such as Internet gambling sites and material on euthanasia or encouraging eating disorders.[155] The testing plan for the second phase of trials includes evaluations of a filtering product's capability to prevent circumvention, which implies blocking sites (such as proxy servers and anonymizers) that enable bypassing restrictions.[156] Yet the Labor government has not openly discussed banning this additional category of sites.

The uncertainty in what material will be proscribed generates at least two transparency problems. First, the government has yet to indicate even the categories of material that it will filter, let alone the criteria by which it will evaluate a site. This makes it difficult for Australian citizens to decide whether the scope of the filtering system is appropriate, overly broad, or insufficient. Minister Conroy's statement about a block list of 10,000 sites suggests either that the government has a sense of the scope of its incipient filtering—though it has not fully shared it with the public—or that he is guessing. The latter seems more likely, particularly given difficulties estimating how many sites in a certain category even exist. Australian Internet companies have picked up on this vagueness in Labor's plans, with the carrier relations manager at the ISP Internode stating that, "we haven't got a clear explanation as to what the Government's actual mandatory blacklist looks like."[157] Attempts to compel the government under Australia's Freedom of Information Act to reveal the contents of its current, more limited ACMA blacklist failed, as the country successfully argued that disclosure would undermine law enforcement

[154] *See, e.g.*, Bryant, *supra* note 94 (indicating that child pornography will be blocked in Australia).

[155] *Senator Conroy Expands Reach of Net Filters to "Unwanted Content,"* IT NEWS AUSTRALIA, Nov. 13, 2008, http://www.itnews.com.au/News/88908,senator-conroy-expands-reach-of-net-filters-to-unwanted-content.aspx.

[156] DEP'T OF BROADBAND, COMMC'NS AND THE DIGITAL ECON., *supra* note 117, at 3.

[157] Asher Moses, *Net Filters May Block Porn and Gambling Sites*, WATODAY, Oct. 27, 2008, *available at* http://www.watoday.com.au/technology/biz-tech/net-filters-may-block-porn-and-gambling-sites-20090616-ce9y.html (quoting John Lindsay).

efforts.[158] Disclosure of the blacklist itself remains illegal,[159] though a purported copy of it is available on the website Wikileaks. This uncertainty is in sharp contrast to restrictions on offline content, where the government publishes categories of banned material.[160]

Second, and more troubling, is that the lack of transparency about what Internet content will be off-limits to Australians prevents them from evaluating how well this blocking relates to the Rudd government's rationales for filtering (as assessed above, under Openness). The primary reason for engaging in mandatory access restrictions, according to the Labor Party, is to protect children. The classification scheme developed under the Broadcasting Services Amendment is tailored—if inconsistently at times—to this end.[161] However, making content that might be harmful to minors, yet lawful for adults, inaccessible in all circumstances runs afoul of the child-protection rationale. This suggests that the government may be adopting, willingly or based upon political calculations, a broader filtering rationale that seeks to prevent harm to adults themselves or to community mores.[162] Such reasons are defensible, but are not the ones upon which Labor was elected. In short, the Rudd government's inability, or unwillingness, to elucidate a consistent set of content categories that will be off-limits, either to all Australians or to minors, undermines citizens' ability to compare concrete plans for filtering to the reasons for implementing it initially.

[158] Electronic Frontiers Australia, FOI Request on ABA, *supra* note 69.

[159] *See generally* ACMA, ACMA LIST OF PROHIBITED AND POTENTIALLY PROHIBITED OVERSEAS HOSTED CONTENT, Mar. 19, 2009, http://www.acma.gov.au /WEB/STANDARD/pc=PC_311669.

[160] *See Conroy Statement*, *supra* note 146 (indicating governmental categories and priorities in banning material).

[161] *See generally supra* notes 56–68 and accompanying text (providing background on the classification scheme).

[162] *See Testimony Before the Senate Standing Committee on Environment, Communications., and the Arts*, *supra* note 145. The Family First Party, for example, advances Internet filtering as a child-protection measure. *See* FAMILY FIRST, PROTECTING CHILDREN FROM PORNOGRAPHY (2008), http://www.familyfirst.org.au /policy/policypornography.pdf (last visited Dec. 4, 2009) (providing a discussion of this position). However, it justifies tightening standards for content allowed on television because shows such as *Big Brother* "legitimiz[e] behavior that is completely unacceptable," contravening "decent standards." FAMILY FIRST, ENSURING DECENT STANDARDS ON TELEVISION (2008) (last visited Dec. 4, 2009), http://www.familyfirst.org.au/policy/policytelevisionstandards.pdf.

The government appears to recognize shortcomings in the transparency of its filtering proposal. Minister Conroy suggested implementing review of the ACMA blacklist, either by an expert panel or by a parliamentary committee, to improve transparency.[163]

At this stage, Australia's transparency regarding its incipient filtering is poor.[164]

5.3. Narrowness

While Australia's filtering system is not yet in place, the first pilot test allows an early estimate of narrowness. Depending upon the filtering product that ISPs deploy (assuming the government does not mandate one method), Australia's censorship could fare quite well or rather poorly on the narrowness criterion. The products varied in how successfully they blocked prohibited content, and only that content. The products' failure to prevent access to some sites banned by Australia is puzzling, but likely stems from relying on vendors' block lists rather than the ACMA's list. This choice—creating a custom block list, or relying on the products' classification schemes—has critical implications for the narrowness, accountability, and ease of implementation of Australia's filtering system. Overall, the country is likely to follow the trend towards over-blocking present in most filtering countries, both to prevent circumvention and to avoid under-blocking.

Filtering systems inevitably block both too much information (over-breadth) and too little information (under-breadth)—they fail to prevent access to some proscribed information, yet also filter material that is permitted. Evaluating narrowness requires examining failure rates on both components, accepting that perfection is unlikely. For over-breadth, the results from the first Tasmanian test of filtering products varied from good (1.3% of innocent sites blocked) to poor (7.8% of such sites blocked).[165] For under-breadth, Australia's system performed moderately well: five

[163] Dan Harrison, *Review of Website Blacklist in Wind*, SYDNEY MORNING HERALD, May 27, 2009, *available at* http://www.smh.com.au/news/technology/web/review-of-website-blacklist-in-ind/2009/05/26/1243103573711.html.

[164] *See generally* AUSTRALIAN COMPUTER SOC'Y, *supra* note 88, at 5 (calling on the Australian government to "establish greater transparency and accountability in the criteria and processes for incorporating sites onto the black list").

[165] AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY, *supra* note 8, at 62–68.

of the six tested products blocked more than 90% of targeted URLs.[166] (Compare this, though, with Iran's success rate of almost 100% in blocking access to pornography.[167])

It is unclear why the tested products failed to block banned sites, and whether this outcome has any implications for full-scale implementation. The ACMA report does not describe precisely how filtering was implemented—it details the different categories of URLs tested, but crucially does not indicate how the products were configured to block them.[168] If the test simply fed the URL lists for Categories 1 and 2 (the prohibited sites) into a block list for each product, the filtering technologies should have achieved 100% success, which means that preventing access to a given URL would be trivial. Thus, it is more likely that the test did not check a product's ability to implement a block list, but rather how well its filtering system detected and blocked sites that Australia deems unlawful or problematic.

For example, if Australia decided to use Secure Computing's SmartFilter product, it could block access to pornographic sites on the ACMA's list in two ways. First, it could configure SmartFilter to block URLs that Secure Computing classifies as Pornography.[169] Indeed, ISPs such as Webshield have lobbied for this option based on effectiveness and performance benefits.[170] Second, Australia could create its own list of prohibited URLs and configure SmartFilter to block them.[171] In fact, the two methods could be combined, at some risk of redundancy. Relying upon a vendor's filtering database or categories is easier for a country such as Australia, since the government or ISPs do not have to manually update block lists, but has the drawback of conferring decision-making power over what constitutes "pornography" or other

[166] *Id.*

[167] OPENNET INITIATIVE, IRAN (June 16, 2009) http://opennet.net/research/profiles/iran (last visited Dec. 4, 2009).

[168] AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY, *supra* note 8, at 20–22, 35–37.

[169] *See* MCAFEE: TRUSTEDSOURCE WEB DATABASE REFERENCE GUIDE 59 (2009), *available at* http://www.securecomputing.com/techpubs_download.cfm?id=2066 (describing pornography category and giving sample URLs).

[170] *See generally* Foo, *supra* note 43 (discussing ISP and Webshield's activities).

[171] *See* SECURE COMPUTING, SECURE WEB FILTER: PRODUCT OVERVIEW 1 (2008), *available at* http://www.securecomputing.com/pdf/WEBW-URLfltr-PO.pdf ("Add your own entries to any one of Secure Web Filter's categories or create and populate your own user-defined categories.").

banned content upon the filtering vendor or other third-party block list provider. It is likely that Australia's pilot project used the first method (using vendors' classification schemes), but not the second, in evaluating filtering products. If the trial sought to block access to a custom URL list—for example, the ACMA's blacklist—it would be surprising if the filtering products failed to achieve complete effectiveness. However, if, Australia should decide to configure filtering to block only URLs specified by the ACMA, narrowness should improve dramatically when censorship is implemented country-wide: current filtering products should block specified URLs, and only those URLs, with perfect accuracy (absent transient technical problems).[172]

While this technical discussion may seem abstruse, it has important implications for how Australia's filtering will work. If the government requires ISPs to block only sites that the ACMA classifies as banned, then both under-blocking and over-blocking should vanish: providers can easily configure their networks to reject attempts to reach a specified list of prohibited URLs. If filtering employs vendor-supplied block lists, or allows ISPs to choose which product to implement (so long as it censors sites on the ACMA list with reasonable reliability), then Australia's controls will inevitably be both under-broad and overbroad, with negative implications for access to legitimate information, transparency, and accountability. A further problem is that filtering, to avoid allowing access to prohibited content, must invariably move towards over-blocking. This is particularly true for sites that enable circumvention of filtering, such as anonymizers, proxy servers, and even language translation sites.[173] Some sophisticated users will employ these seemingly innocent sites to access banned material.[174] A filtering government must then decide between allowing some (likely low) level of access, or expanding blocking to cover sites that are nominally licit but that can bypass censorship. Similarly, it may be necessary to block certain ports and Internet protocols, such as SOCKS[175] or virtual

[172] *See generally* Foo, *supra* note 14.

[173] *See generally* Villeneuve, *supra* note 96 (discussing the problems these websites create).

[174] *See* CITIZEN LAB, *supra* note 101 (describing how this occurs).

[175] *See* Contempt, *supra* note 97 (stating explicitly the weaknesses in the proposed filtering system).

private networks,[176] to prevent users from employing other circumvention techniques. Indeed, Australia's technical specifications for the second set of tests state that it "will involve common circumvention techniques (e.g. use of proxies) and the measures that a filtering solution has in place to address these."[177] Australia is clearly contemplating blocking or preventing circumvention. To be effective, censorship must often target sites that bear no direct relation to the material that a country purports to ban. This creates collateral harms, as users may not be able to use Google's cache or translation sites.

To most effectively prevent access to prohibited sites, filtering countries must generally accept over-blocking. The Tasmanian test results illustrate this general trend: methods that are more effective in preventing access to banned material also tend to catch more unrelated sites in their filters. Nations that implement filtering in a non-symbolic way—Singapore, for example, blocks only a few sites as a gesture of disapproval [178]—often tolerate over-breadth as the price of preventing access to illicit content.[179] Australia faces a similar choice: the tested product with the greatest success in walling off banned sites (lowest under-breadth) had the second-worst record in blocking permissible ones (second-highest over-breadth), while the tested solution with the lowest level of inadvertent filtering also missed the most prohibited sites.[180]

Filtering Product	**% Prohibited URLs Blocked**	**% Permissible URLs Blocked**
Alpha	90	2.6
Beta	**98**	**7.5**
Gamma	**87**	**1.3**
Delta	91	2.4

[176] *See* Hendry & Pauli, *supra* note 3 (giving an example of how a private network was used for a circumvention technique).

[177] DEPARTMENT OF BROADBAND, *supra* note 117, at 6.

[178] *See* OPENNET INITIATIVE, SINGAPORE 3 (2007) http://opennet.net/research /profiles/singapore (2007) (documenting that Singapore's ISPs block only seven pornographic sites).

[179] *See, e.g.*, OPENNET INITIATIVE, SUDAN 4 (2007) http://opennet.net/studies /sudan2007 (2007) (describing that a search portal and a site on domestic violence had been previously misclassified as pornography and blocked).

[180] AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY, *supra* note 8, at 62–68.

Theta	94	7.8
Omega	94	2.9

TABLE 2 – OVER-BREADTH / UNDER-BREADTH FROM FILTERING TRIAL[181]

Perfect censorship is a myth: banned information inevitably leaks through filters, and blocking always strains out wheat along with chaff. The results from Australia's pilot program indicate that its filtering narrowness could be strong or poor, depending on the product employed. The tradeoff that the country and its ISPs select, and the resulting balance between over-blocking and under-blocking, will do much to illuminate the government's value choices.

5.4. Accountability

Formally, Australia's censorship decision makers are highly accountable to citizens, yet there are subtle but important concerns. Labor's dependence on minority parties in the Senate can confer disproportionate power upon senators with strong views on filtering that appear out of step with majority public opinion. The government has moved to silence some dissenters, and is considering using block lists developed by foreign entities with no accountability and with potentially differing standards for content classification. Filtering itself confers considerable power on those who implement it (such as ISPs) and design it technologically (such as software vendors), and makes later expansion of censorship easier by reducing the cost of blocking additional content.

Accountability encompasses a range of ways by which citizens can participate in filtering decisions. This can happen directly, as when users in Saudi Arabia request that a website be blocked or unblocked,[182] and also indirectly, as when citizens vote for politicians who carry out their preferences. Ordinarily, Australia should score high for accountability: the country has a robust

[181] *Id.*

[182] Robin Miller, *Meet Saudi Arabia's Most Famous Computer Expert*, NEWSFORGE, Jan. 14, 2004, http://www.linux.com/archive/articles/33695. *See generally* ABDULAZIZ HAMAD AL-ZOMAN, THE INTERNET IN SAUDI ARABIA (TECHNICAL VIEW) (2001), http://www.isu.net.sa/library/CETEM2001-Zoman.pdf (presenting data on the internet in Saudi Arabia).

democracy, independent judiciary, written constitution, protections for minority groups, and other features of a Western democracy.[183] Indeed, the government's responsiveness to public opinion is arguably stronger in Australia's parliamentary democracy than in the United States' republican one: Australian governments unable to command a majority in parliament face a near-immediate test at the polls, while U.S. elections occur at regular intervals regardless of the particular government's support. To its credit, the Rudd government has shown a willingness to consider feedback on its Internet policies, even from skeptics: the chief executive of the Internet Industry Association ("IIA"), who has criticized the filtering proposal, was named to the new Cyber-Safety Consultative Working Group promised under Labor's election platform.[184] There are, however, several worrisome issues regarding accountability in the filtering context.

One issue is that the Labor government's policy has shifted in the direction of expanding blocking since the election in two ways. First, the government seeks to make some blocking (the first tier of the system) mandatory for all Australians, although its platform indicated that adults could opt out of such restrictions. The government's lack of transparency regarding its plans makes it harder to hold Labor to account for any such shift. Second, the scope of material targeted has broadened. This may represent the policy goals of Minister Conroy or the Rudd government, but the change also moves Labor closer to minority parties that advocate wider bans, such as Family First. This situation creates the possibility of undue influence by a minority over the majority of voters.

Another concern is that the government appears to be seeking to suppress dissent in some cases.[185] Mark Newton, an employee of the ISP Internode, has actively opposed the filtering plan in posts to newsgroups and online forums.[186] (Newton makes clear

[183] *See generally Country Profile: Australia*, BBC NEWS, http://news.bbc.co.uk /2/hi/asia-pacific/country_profiles/1250188.stm#facts (providing general information about Australia and its leaders).

[184] *Big Core*, CANBERRA TIMES, May 19, 2008, at A13; Press Release, Senator Stephen Conroy, Consultative Working Group to improve Cyber-Safety (May 15, 2008), http://www.minister.dbcde.gov.au/media/media_releases/2008/035.

[185] *See generally* Hendry & Pauli, *supra* note 3.

[186] *See, e.g.*, Posting of Mark Newton to http://forums.whirlpool.net.au / forum-replies.cfm?t=967413&r=16774529#r16774529 (Sept. 30, 2008, 4:58 PM) (posting in opposition to the filtering plan).

that he does not speak for his employer.)[187] Belinda Dennett, policy advisor to Minister Conroy, sent an e-mail message to the IIA stating her "serious concern that a [sic] IIA member would be sending out this sort of message."[188] Furthermore, Minister Conroy has suggested that opponents of the filtering program support child pornography.[189] While hyperbolic rhetoric is common in democracies, attempts to silence dissenters or to conflate policy differences with support for unlawful behavior undermine accountability.

The government has also suggested it will expand ACMA's block list by adding sets of problematic URLs from foreign entities that seek to combat child abuse, such as the Internet Watch Foundation.[190] This would mean that entities that are not accountable to Australian voter and applying standards other than those set by Australia law, would decide what Internet material is off-limits in the country. While the accountability problem would be reduced if the ACMA and Classification Board independently assessed the content on the foreign block lists, treating third-party block lists as complaints would likely run afoul of the statutory scheme under which the ACMA operates.[191]

Moreover, filtering itself creates two fundamental accountability problems. First, online censorship using technology confers significant power on both the entity implementing filtering (such as an ISP) and the entity designing it (such as software vendors Websense[192] and Secure Computing).[193] In Australia's case, it appears that ISPs may be able to choose among different

[187] *See, e.g.*, John Timmer, *Aussie govt: Don't Criticize Our (Terrible) 'Net filters*, ARS TECHNICA, Oct. 24, 2008 (on file with U. Pa. J. Int'l L.) (criticizing the Australian government's filtering policy).

[188] Asher Moses, *Filtering Out the Fury: How Government Tried to Gag Web Censor Critics*, THE AGE (Melbourne), Oct. 24, 2008, http://www.theage.com.au/articles/2008/10/23/1224351430987.html?page=2.

[189] *Conroy Announces Mandatory Internet Filters to Protect Children*, *supra* note 115 (quoting Conroy: "If people equate freedom of speech with watching child pornography, then the Rudd-Labor Government is going to disagree").

[190] *See supra* notes 79–86 and accompanying text.

[191] *See supra* note 82 and accompanying text.

[192] *See* Websense Web Filter, http://www.websense.com/content/WebFilter.aspx (last visited Dec. 4, 2009) (providing information for the Websense filtering product).

[193] *See* McAfee SmartFilter, http://www.securecomputing.com/index.cfm?skey=85 (last visited Dec. 4, 2009) (describing the benefits and features of McAfee SmartFilter).

products that can censor the Web.[194] This could enable ISPs to offer filtering Internet access of varying narrowness, all within the statutory scheme set forth by the government.

If Australia's ISPs use the block lists created by these products' vendors, this will transfer important normative decisions about classifying and filtering content from Australia's government, which is accountable, to private companies—which may not be Australian in origin or location—that are not. Australia has a detailed legal framework for determining what content is, and is not, subject to prohibition. If filtering is implemented based on software vendors' decisions about whether content is sexually explicit, rather than on ACMA's or the Classification Board's judgments, this decreases citizens' ability to have a voice in what they can access online. This accountability challenge may also be convenient for decision makers, as it lets them displace grievances over blocking decisions onto technology companies and portray problems as technical in nature rather than reflecting a deliberate normative choice. To improve accountability, the Labor government should disclose how it plans to implement filtering at the ISP level, including the process by which a site is selected for blocking and how that restriction is implemented at a technical level. This will enable Australian citizens to decide whether the government's plan comports with their own views on filtering, and to make those views known at the polls.

Second, once censorship is implemented, the costs and difficulties of blocking additional content are greatly reduced. Should the Labor government decide to block sites about illegal drugs, for example, it could do so using some filtering products simply by selecting an additional category as prohibited.[195] This creates not only a slippery slope problem—once initial reluctance to censor is overcome, additional steps may appear less weighty—but can also make it difficult to determine precisely what content is blocked, and why. [196]

[194] *Cf.* DEPARTMENT OF BROADBAND, *supra* note 117, at 2–3.

[195] *See, e.g.*, Secure Computing, http://www.securecomputing.com /index.cfm?skey=86#categories (describing the drugs category of sites blocked by smartfilter).

[196] *Cf.* Hendry, *supra* note 3 (pointing out that a content filtering scheme installed in Parliament offices mistakenly blocked legitimate topics like gun control and breastfeeding).

Accountability problems are inherent in censorship achieved through computer technology. These challenges increase when some voices are magnified, and others silenced, in policy debates, and when content categorization is done by unaccountable (and perhaps foreign) entities. How Australia implements filtering will influence the control its citizens have over online content restrictions.

6. CONCLUSION

Australia is moving to censor the Internet because the Labor Party won office partly on a promise to do so. The country will likely become the first Western democracy to block access to online material through legislative mandate, creating a natural experiment. However, this experiment raises concerns. The government has not been clear about what material will be blocked, and why. The censorship system's accountability to citizens could be undercut by the combined effects of pressures to win Senate passage of legislation, outsourced content classification, and filtering's inevitable transfer of power to those who design and implement its technology. Results from the first test of filtering should be a cautionary tale, guiding not just the technical deployment of censorship, but also highlighting political, social, and Internet policy issues that must continue to be vigorously debated.

Australia's decision to censor Internet content preemptively is further evidence that the debate over filtering has shifted, from whether filtering should occur to how it should work. Cyberlibertarianism is alive and well, as discussions in Australia's press and Parliament prove, but it is no longer ascendant. This shift disguises an important change in focus for regulating information. Filtering looks easy and cheap, and calls to block access to material that is almost universally condemned—such as child pornography, extreme violence, or incitements to terrorism—are hard to resist. But this focus confuses means with ends. The key question is what set of measures best achieve the end, or combat the evil, at issue—and how tolerable their countervailing drawbacks will be. Democratic governance is well-positioned to debate these tradeoffs, and indeed Australia's move is less worrisome than filtering in, for example, Great Britain, which implemented censorship through "voluntary" agreements between ISPs and government. The concern is that as filtering is increasingly adopted in Western democracies, censorship that blocks access to material rather than legal measures that punish access after the fact will become increasingly seen as normal rather than problematic. As this Article, and other work on filtering by groups such as the OpenNet Initiative demonstrate, filtering carries considerable costs in over-blocking, transparency, and accountability that may not be evident initially. Censorship can be an effective tool, but it is a dangerous one. Australia's example will have much to teach about both aspects.