Untangling the Web: Exploring Internet Regulation Schemes in Western Democracies

RENEE KEEN*

TABLE OF CONTENTS

---

* J.D. Candidate 2012, University of San Diego School of Law. I would like to thank Professor Junichi P. Semitsu and the members of the editorial board of the *San Diego International Law Journal* for their invaluable guidance in drafting and editing this Comment. I would also like to thank Christopher Dirscherl for his patience and support.

I. INTRODUCTION

In January 2010, research by the OpenNet Initiative[1] revealed that more than half a billion of all Internet users worldwide are currently being censored.[2] Thirteen nations currently employ "pervasive filtering,"[3] seven additional nations employ "substantial filtering,"[4] and roughly thirty-six nations employ some varying degree of "nominal filtering."[5]

Most discussions about Internet censorship focus heavily on repressive regimes,[6] and while "focusing on these ugly regimes is popular, it can blind us to other developments."[7] Censorship is no longer a tactic reserved for authoritarian administrations interested in silencing political dissent. Internet censorship has now become a method explored by democratic nations seeking to regulate illegal activities conducted online.[8]

The task of developing a workable filtration system has proven difficult, and often futile, in democratic nations as a result of the watchful eyes of concerned citizens and civil liberties organizations. Although

1. OpenNet Initiative (ONI) is a collaborative partnership of three institutions: the Citizen Lab at the Munk School of Global Affairs, University of Toronto, the Berkman Center for Internet & Society at Harvard University, and the SecDev Group (Ottawa). ONI investigates and analyzes Internet surveillance and filtering practices across the globe. *See* OpenNet Initiative, *About Oni* (Jan. 2010), http://opennet.net/about-oni.

2. Jillian C. York, *More than half a billion Internet users are being filtered worldwide*, OPENNET INITIATIVE (Jan. 2010), http://opennet.net/blog/2010/01/more-half-a-billion-internet-users-are-being-filtered-worldwide [hereinafter ONI].

3. Pervasive filtering is defined by ONI as "characterized by both its depth—a blocking regime that blocks a large portion of the targeted content in a given category—and its breadth—a blocking regime that includes filtering in several categories in a given theme." *See id.* at 112.

4. Substantial filtering is defined by ONI as "[having] either depth or breadth: either a number of categories are subject to a medium level of filtering, or a low level of filtering is carried out across many categories." *Id.*

5. Nominal or selective filtering is defined by ONI as "narrowly targeted filtering that blocks a small number of specific sites across a few categories or filtering that targets a single category or issue." *Id.*

6. This assertion is evidenced by two LexisWeb Searches: the first search "internet censorship" AND "China" yielded 31,446 results (last visited Aug. 31, 2011) while the second search "internet censorship" AND "democracy" yielded only 23,036 results (last visited Aug. 31, 2011).

7. Robert Boorstin, Google Director of Corporate and Policy Communications, Address at the Geneva Summit for Human Rights Tolerance and Democracy (Mar. 9, 2010) (transcript available at http://blog.unwatch.org).

8. Joshua Keating, *The List: Look Who's Censoring the Internet Now*, FOREIGN POLICY (Mar. 4, 2009), http://www.foreignpolicy.com/articles/2009/03/23/the_list_look_whos_censoring_the_internet_now?page=0,0.

proposals in many democratic nations have been criticized and stagnated as a result of the stigma associated with censorship, it is apparent that new proposals will continue to surface through governments eager to curtail illegal activities otherwise capable of flourishing with impunity in the robust cyber realm.[9]

This Comment investigates past censorship schemes proposed and implemented by selected democratic administrations, in order to develop an improved framework and accompanying infrastructure that may accomplish the goals that these policies envisioned, but failed to achieve.[10] The difficulty of this undertaking is in developing the intermediate and legally defensible parameters under which a regulation scheme can endure and gain support in a democratic society. The greater difficulty lies in developing a system that can accomplish these objectives in the burgeoning and ever-changing cyber realm.

The challenges posed by Internet activity are novel ones, and the legitimacy of the actions taken in response is equally uncertain.[11] This Comment examines the "first wave" of censorship approaches that have been drafted, proposed, and adopted by democratic nations, focusing on Australia, the United States, and the United Kingdom. By evaluating the censorship policies proposed by each of these nations, this Comment identifies and examines the successful as well as the ineffectual elements of each of these policies, in order to develop general guidelines under which a democratic Internet regulation scheme may one day legitimately operate.

---

9. *See United States and Canada.* OPENNET INITIATIVE (2010), http://opennet.net/research/regions/namerica.

10. The primary focus of this comment is not on censorship targeting copyright infringement online. For a discussion of this and related issues see Graeme W. Austin, *Social Policy Choices and Choice of Law for Copyright Infringement in Cyberspace*, 79 OR. L. REV. 575 (2000). *See also* Peter S. Menell, *Can our Current Conception of Copyright Law Survive the Internet Age?: Envisioning Copyright Law's Digital Future*, 46 N.Y.L. SCH. L. REV. 63 (2002–03).

11. "[T]he use of technology to exert control over internet users frequently challenges tenets associated with the rule of law concerning both the process for and content of norms governing behavior." T. J. McIntyre & Colin David Scott, *Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility*, *in* REGULATING TECHNOLOGIES 109, 111 (R. Brownsword & K. Yeung, eds., Oxford, Hart Publishing 2008).

II. BACKGROUND

Crimes committed with the aid of the Internet are on the rise,[12] as is the number of nations responding by developing and adopting Internet censorship policies.[13] In recent years, governments around the world have been confronted with the difficult and complex issues that arise when attempting to develop methods with which to monitor and restrict the spread of harmful, and often illegal, content on the Internet.[14] While all governments have been faced with novel complications posed by the prevalence of the World Wide Web, democratic nations have had to confront the uniquely difficult matter of balancing the need to regulate illegal material, while simultaneously preserving the inherently democratic freedoms upon which they are built.[15]

The Internet and its various forms of information spreading, pose special, unprecedented difficulties for governments attempting to restrict access to illegal, harmful, and in some cases, politically dissenting content. Due to the unique nature of these threats and the unparalleled nature of the medium with which they are spread, governments have attempted to reconcile their inability to control or punish the content hosted overseas by adopting filtering policies that enable them to prevent this content from being accessible to their citizens.[16] Attempts to regulate content hosted abroad have been emerging in various formats, and in order to be effective, have all incorporated some form of cooperation from Internet service providers (ISPs), whether through legal mandate[17] or informal pressure.[18]

---

12. Janis Wolak, *Trends in Arrests of Online Predators*, CRIMES AGAINST CHILDREN RESEARCH CTR. 1, 2 (2009), *available at* http://www.unh.edu/ccrc/pdf/CV194.pdf.

13. ONI, *supra* note 2.

14. *Internet Censorship*: *Law & Policy Around the World*, ELECTRONIC FRONTIERS AUSTRALIA [EFA], http://www.efa.org.au/Issues/Censor/cens3.html (last updated Mar. 28, 2002).

15. *See generally* John G. Palfrey, Jr. & Robert Rogoyski, *The Move to the Middle: The Enduring Threat of "Harmful" Speech to the End-to-End Principle*, 21 WASH. U. J.L. & POL'Y 31 (2006) (describing recent changes in Internet regulation practices).

16. Mary Rundle & Malcolm Birdling, *Filtering and the International System: A Question of Commitment*, *in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 73, 90 (Ronald J. Deibert et al. eds., 2008).

17. *See generally* Jennifer Dudley-Nicholson, *Australia's Compulsory Internet Filtering "Costly, Ineffective,"* THE COURIER-MAIL, (Oct. 29, 2008), http://www.news.com.au/technology/story/0,25642,24569656-5014239,00.html.

18. *See* Frank Fisher, *Caught in the Web*, THE GUARDIAN (Jan. 17, 2008), 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).

A. How the Internet Differs from Its Predecessors

There are a multitude of characteristics that differentiate "online media" from its predecessors of print and broadcast media. The pervasiveness of the Internet has grown at an unprecedented rate.[19] The world population was an estimated 6.93 billion as of March 2011, of which an estimated 2.096 billion Internet users.[20] From 2000 to 2011, Internet usage among the world's population increased by an astonishing 480.4%.[21]

In addition to its universal prevalence, the Internet has enabled new forms of human interaction as a result of the ease and speed with which information can be accessed and spread across the globe.[22] In 1798 it took 62 days for news of the Battle of Nile[23] to travel 2,073 miles in order to reach London.[24] This information traveled across the globe at a speed of 1.4 miles per hour.[25] Nearly a century later, in 1891, it took only one day for news of the Nobi Earthquake in Japan to travel 5,916 miles in order to reach London, attaining a speed of 246 miles per hour.[26] Today, this information can travel across the globe almost instantaneously.[27]

Access to the Internet is currently available through a myriad of devices and electronic hardware, including desktop computers, laptops, mobile phones, and various other handheld devices. With each new device comes

---

19. *Internet Usage Statistics the Internet Big Picture*, INTERNET WORLD STATS, *available at* http://www.internetworldstats.com/stats.htm (last updated Feb. 14, 2011).
20. *Id.*
21. *Id.*
22. *See infra* notes 23–27 and accompanying text.
23. Battle of the Nile was a major naval battle fought between British and French fleets during the Napoleanic Wars. This battle in Aboukir Bay, Egypt marked one of the greatest British victories of Admiral Horatio Nelson, in defeating French Revolutionary general Napoleon Bonaparte. *See Battle of the Nile*, ENCYCLOPÆDIA BRITANNICA ONLINE, http://www.britannica.com/EBchecked/topic/415322/Battle-of-the-Nile (last accessed Nov. 15, 2010).
24. GREGORY CLARK, A FAREWELL TO ALMS, Table 15.3: 1798–1914, *Speed of Information Travel to London*: chart (2007), *available at* http://beebo.org/lately/2009-07-12_speed-of-information-travel.html.
25. *Id.*
26. *Id.*; Jason Kottke, *The Speed of Information Travel, 1798–2009*, KOTTKE (Sept. 2009), http://kottke.org/09/09/the-speed-of-information-travel-1798–2009.
27. While the Internet is the newest medium for the flow of information, it is the fastest growing communication medium of all time. It is therefore, unsurprisingly, the first resort for information access for many of its users. *See* Peter Lyman & Hal R. Varian, *How Much Information?* (2003), http://www.sims.berkeley.edu/how-much-info-2003/execsum.htm.

an easier and more convenient method of accessing the Internet. Two thirds of the world's population currently has access to mobile phone technology, making it the fastest spreading technology in human history.[28] This statistic, coupled with predictions by leading information technology analysts that "mobile phones will overtake PCs as the most common web access device" by the year 2013, emphasizes the astonishing implications of modern technology.[29]

The Internet provides anyone with access the ability to publish content online with little or no oversight.[30] To emphasize the extent of the publication capability facilitated by the Internet, consider this: "[e]very minute, 20 hours of video is uploaded to YouTube."[31] Furthermore, the Internet greatly enables, if not encourages, its contributors to participate anonymously.[32] The danger posed by this new era of information technology spread is that all information, good and bad, helpful and harmful, has the potential to spread virally.[33] With increased speed, accessibility, and participation comes a greater risk of uncontrollable information spread, and a more complicated task for governments seeking to restrict access to illegal, harmful, or otherwise inappropriate content.[34]

Perhaps it is time for democratic citizens to recognize Internet filtration as a viable method for ensuring that the activities and materials easily recognizable as illegal by offline laws are capable of being similarly identified and punished in the far more complicated online realm.

B. The Unique Challenge of Censorship in a Democracy

Notwithstanding the disparate objectives of authoritarian and democratic nations in constructing policies to respond to the threat posed by the prevalence of the Internet, democratic nations face a more complex challenge in developing and implementing policies to respond to this

---

28. Boorstin, *supra* note 7.

29. Brian Gammage, *Gartner Top Predictions for 2010 Coping with the New Balance of Power*, GARTNER WEBINAR, Slide 6 (2009), *available at* http://www.gartner.com/it/content/1260200/1260221/january_14_top_predictions_2010bgammage.pdf.

30. Note that this paragraph is intended to emphasize the ease of publication on the Internet generally. The ability to publish freely or anonymously is restricted under certain authoritarian regimes. China, for example, has banned anonymous cell phone purchases. *See* Brian Barrett, *China Bans Anonymous Cell Phone Purchases*, GIZMODO (Sept. 9, 2010, 8:40 PM), http://gizmodo.com/5634304/china-bans-anonymous-cellphone-purchases.

31. Boorstin, *supra* note 7.

32. Kenny Silverman, *Defamation on the Internet*, 601 PLI/PAT 327, 333 (2000).

33. Harold Smith Reeves, *Property in Cyberspace*, 63 U. CHI. L. REV. 761, 765 (1996).

34. *Id.*

threat.[35] The censorship measures taken by non-democratic nations in response to information deemed harmful on the Internet are not capable of being closely monitored through similar measures taken by democratic nations.[36]

The Chinese government, for example, has reserved for itself the right to silence dissenters, such that the consequences of taking steps to prevent the spread of unfavorable information on the Internet are minimal within its borders.[37] In addition, authoritarian leaders are not politically accountable to their populations in the manner that democratic governments are.[38] Repressive censorship policies are largely criticized outside of these nations,[39] but the lack of transparency,[40] and continued cooperation from mega corporations,[41] have placed efforts by democratic nations to discourage repressive censorship at a standstill.

Democratic nations have more difficulty dealing with new threats posed by the Internet because the tenets of democracy and the freedom of expression prohibit governments from making unilateral decisions to restrict speech and other inherent freedoms.[42] In addition, democratic governments can be openly criticized because criticism and political dissent are essential to the functionality of a democracy.[43] These factors, combined with the accountability of the government to its citizens, have

35. Derek E. Bambauer, *Cybersieves*, 59 DUKE L.J. 377, 384 (2009).

36. *Id.* at 401.

37. *See* Michael Sainsbury, *China Cracks Down on Dissenters*, THE AUSTRALIAN (May 11, 2010), http://www.theaustralian.com.au/news/world/china-cracks-down-on-dissenters/story-e6frg6so-1225864742031; *see also* Peter Beaumont, *Why is China So Terrified of Dissent?*, GUARDIAN NEWS & MEDIA LTD. (Jan. 17, 2010), http://www.guardian.co.uk/world/2010/jan/17/china-terrified-dissent-dissident-chinese; *see also* Ben Doherty, *Silence of the Dissenters: How South-East Asia Keeps Web Users in Line*, GUARDIAN NEWS & MEDIA LTD. (Oct. 21, 2010), http://www.guardian.co.uk/technology/2010/oct/21/internet-web-censorship-asia?intcmp=239.

38. Bambauer, *supra* note 35 at 406-07.

39. OFFICE OF THE U.S. TRADE REPRESENTATIVE, 2008 SPECIAL 301 REP. 7, *available at* http://www.ustr.gov/sites/default/files/asset_upload_file553_14869.pdf (criticizing the Chinese search engine Baidu).

40. Nart Villeneuve, *Search Monitor Project: Toward a Measure of Transparency* 1, 7 (Citizen Lab, Occasional Paper No. 1, 2008), http://citizenlab.org/wp-content/uploads/2011/08/nartv-searchmonitor.pdf.

41. *See* Stuart Biggs, *Under Oath and Under Pressure*, S. CHINA MORNING POST, Feb. 21, 2006, at 1.

42. Some corporations have continued to comply with censorship policies in pursuit of business incentives. *See* Bambauer, *supra* note 35 at 403.

43. In fact, democratic leaders such as President Barack Obama encourage criticism and accountability. *See infra* note 193 and accompanying text.

posed great challenges for democratic nations in their attempts to respond to the unparalleled level of access to information and material facilitated by the Internet.[44]

III. INTERNET CENSORSHIP IN AUSTRALIA

The current Internet censorship regime in Australia is encompassed by the Broadcasting Services Amendment Act of 1999 (BSA).[45] The BSA is a complaint-based system requiring domestic servers hosting objectionable content to remove the material upon receipt of a takedown notice distributed by the Australian Communications and Media Authority (ACMA).[46] The ACMA is the government regulatory agency responsible for evaluating and responding to complaints filed by Australian Internet users.[47] While participation from citizens is a useful and efficient means of locating and removing inappropriate content, the ACMA is also entitled to initiate investigations independently.[48]

In order for the ACMA to deem content objectionable to the extent that it requires removal, it must qualify as "prohibited" based on the classification system developed by the Australian government.[49] The scope of "potentially prohibited" content has expanded over the years, but today may cover material from the following categories: RC (refused classification), X18 (non-violent, sexually explicit activity between consenting adults), R18 (likely to disturb or harm minors), and, in some instances, MA15+ (restricted audiences).[50] These categories were created by the government's "Classification Board," which has crafted national guidelines for the classification of various forms of media.[51]

---

44. Bambauer, *supra* note 35.

45. *Broadcasting Services Amendment (Online Services) Act 1999*, No. 90 (amending Broadcasting Services Act, No. 110, 1992) (Austl.).

46. *See Broadcasting Services Act 1992*, No. 110, §§ 147, 149 (1992) (Austl.); ACMA, *Prohibited Online Content*, ACMA, *Prohibited Online Content*, http://www.comlaw.gov.au/Details/C2011C00390; EFA, *infra* note 54.

47. EFA, *supra* note 14.

48. *See generally Online Regulation*, ACMA, http://www.acma.gov.au/WEB/STANDARD/pc=PC_90169 (last updated Aug. 13, 2010).

49. ACMA, Prohibited Online Content, http:// www.acma.gov.au/WEB/STANDARD/pc=PC_90102 (last updated July 26, 2011); *see* NATIONAL CLASSIFICATION CODE, FED. REG. OF LEGIS. INSTRUMENTS F2005L00816 (Austl.), *available at* http://www.comlaw.gov.au/Details/F2005L00816.

50. *Australia's Internet Censorship System*, LIBERTUS.NET, (Apr. 11, 2010), http://libertus.net/censor/netcensor.html#sc2008; *see Broadcasting Services Act*, No. 110, §§ 147, 149 (1992) (Austl.); *see also id.*

51. Derek Bambauer, *Filtering in Oz: Australia's Foray into Internet Censorship*, 31 U. PA. J. INT'L L. 493, 502–03 (2009).

The ACMA employs a different approach against domestically hosted content.[52] Material hosted within Australia's borders is forwarded by the ACMA to the Classification Board,[53] which reviews the material and makes a final determination.[54] If the content is ultimately deemed "prohibited," a takedown notice is sent by the ACMA to the ISP (or content host) who is then responsible for removing the content. When material that is not hosted in Australia is classified by the ACMA as "prohibited," the Agency does not forward it to the Classification Board, but rather makes a prediction as to the Board's classification and responds accordingly—either permitting the content to remain or notifying "blocking software vendors to add the site to their block lists."[55] Through a combination of complaints, investigations, and classifications, this system has been utilized to generate the blacklist of sites compiled by the ACMA.[56]

Current Australian Censorship policies have not been implemented in a manner that legally requires ISPs to block access to overseas content; however, they are required to remove objectionable content hosted within their borders.[57] Australian citizens are largely familiar with the current policy, and some were even tolerant[58] while under the impression that this policy was narrowly targeted to combat websites "relating to child sexual abuse, rape, incest, bestiality, sexual violence and detailed

52. *Id.* at 502.
53. *Id.* at 503–04.
54. *Internet Censorship: Internet Censorship Laws in Australia*, ELECTRONIC FRONTIERS AUSTRALIA, http://www.efa.org.au/Issues/Censor/cens1.html (last updated Mar. 28, 2002).
55. *Regulating Online Content*, ACMA, http://www.acma.gov.au/WEB/STANDARD/pc=INT_IND_CONTENT_ABOUT (last visited Feb. 17, 2011).
56. Bambauer, *supra* note 51 at 505.
57. EFA, *supra* note 54.
58. Louisa Hearn, *Study casts doubt over net filter support*, THE SYDNEY MORNING HERALD (May 12, 2010), *available at* http://www.smh.com.au/technology/technology-news/study-casts-doubt-over-net-filter-support-20100512-uvo0.html (discussing how various studies indicated support for internet censorship in the interest of protecting children, but when details of the mandatory filter and possible alternatives were explained, enthusiasm dropped); *Australia to implement mandatory internet censorship*, HERALD SUN (Oct. 29, 2008), http://www.heraldsun.com.au/mandatory-censorship-on-web/story-fna7dq6e-1111117883306 (quoting EFA board member Colin Jacobs, "If the Government would actually come out and say we're only targeting child pornography it would be a different debate.").

instruction in crime"; however, disapproval and strong opposition emerged following two contentious incidents surrounding censorship in Australia.[59]

The onset of opposition from the Australian populace was marked by perhaps the most controversial censorship proposal by a democratic government to date.[60] In 2009, the Australian Labor Party proposed a censorship policy that would legally mandate ISPs to filter and block overseas websites falling into the "refused classification" category.[61] Australian ISPs would be required by law to abide by the aforementioned classification system,[62] refusing access to all users based on this categorization, or face legal repercussions and substantial fines.[63]

Despite the Australian citizenry being familiar with the tools previously employed by the government to enforce blocking—the ACMA and the black list—this sudden forceful opposition has come as a result of the potentially freedom restricting proposal to mandate these allegedly overbroad blockings by law.[64] Because this list would continue to be formulated without any transparency, Australian citizens have finally become truly concerned about the potential consequences.[65] This would

---

59. Rich Bowden, *Whistleblower Site Publishes Internet Blacklist*, THE TECH HERALD (Mar. 19, 2009), http://www.thetechherald.com/article.php/200912/3245/Whistleblower-site-publishes-Internet-blacklist (quote by Australian Senator Steven Conroy about content of existing ACMA blacklist).

60. EFA, *supra* note 54.

61. Internet Service Provider (ISP) filtering frequently asked questions, DEP'T OF BROADBAND COMMC'NS & THE DIGITAL ECON. (DBCDE), (last updated Oct. 11, 2011), http://www.dbcde.gov.au/funding_and_programs/cyber safety_plan/internet_service_provider_isp_filtering/isp_filtering_live_pilot/isp_filtering–frequently_asked_questions#11.0.

62. EFA, *supra* note 14.

63. ISP filtering frequently asked questions, *supra* note 61.

64. Ari Sharp, *Opposition grows to internet filter*, THE SYDNEY MORNING HERALD (Feb. 25, 2010), http://www.smh.com.au/technology/technology-news/opposition-grows-to-internet-filter-20100224-p3ma.html#ixzz1d57HNfHJ ("MP [members of parliament] on both sides of politics opposed to the government's internet filtering proposal are vigorously lobbying their colleagues"); Iarla Flynn, *Our submission on mandatory ISP level filtering*, OFFICIAL GOOGLE AUSTRALIA BLOG (Feb. 14, 2010), http://google-au.blogspot.com/2010/02/our-submission-on-mandatory-isp-level.html ("There has been a lot of attention around the Australian Government's mandatory ISP level filtering proposal. Google--and many of you--have argued that the proposal goes too far, with a broad-scoped filter, and a regime which takes the focus off more important areas such as online safety education and better support for policing efforts."); Media Release, *Joint Statement on Internet Censorship*, SAVE THE CHILDREN AUSTRALIA (July 2009), http://www.savethechildren.org.au/images/documents/Joint_Statement_on_Internet_Censorship.pdf ("No other Western democracy has *mandatory* ISP-level internet filtering. Australians should not have to sacrifice their freedoms to make Australia a world-leader in ineffective Internet censorship." (emphasis added)).

65. *See Australian Internet Censorship Filter Delayed*, UNITE THE COWS: DIGITAL MEDIA RESOURCE (July 13, 2010), http://www.unitethecows.com/content/245-australian-internet-censorship-filter-delayed.html ("After drawing a multitude of complaints from citizens concerned that the system would sensor far more than child pornography, Australian officials have decided to take the next year to refine the system.").

prevent Australians from having any legal means with which to access certain objectionable content hosted overseas, including some information that they may be legally entitled to view.[66]

A global censorship comparison report compiled by the Electronic Frontiers Australian (EFA) asserts "the lack of similar laws in comparable countries is not due to a failure of [other] Parliaments or Governments to consider the problems of illegal content unsuitable for minors on the Internet. Rather, it reflects a different approach from that of Australia to dealing with the problems."[67] "Australia's decision to impose mandatory Internet censorship through technology [filtering] . . . puts the country at the forefront of the spread of this practice from authoritarian regimes such as China and Iran to Western democratic nations."[68]

Some authorities respond to these accusations by contending that there can be no "legitimacy" argument against a government taking actions it is legally entitled to take.[69] Australia does not have a Constitutional equivalent to the First Amendment, and therefore does not recognize the same freedom of expression that serves as broad protection to the United States citizenry against similar policies.[70]

Despite rationalizations citing the atypical nature of Australia's democratic composition, the uneasy response from ISPs demonstrates that Australia is entering into a controversial and potentially illegitimate realm of online censorship.[71] In response to the various stages of proposed legislation, ISPs confronted Australian Parliament with numerous concerns. Google, a mega corporation that previously found itself at the forefront of a censorship controversy with China, voiced certain concerns to Australian Parliament about the proposal.[72] Google submitted a report in which it stated:

---

66. Charles Arthur, *Google and Yahoo Criticise Australia's 'Heavy-Handed' Internet Filter Plans*, THE GUARDIAN (Mar. 29, 2010), http://www.guardian.co.uk/world/2010/mar/29/google-yahoo-australia-internet-filter.

67. EFA, *supra* note 14.

68. Karina Travaglione, *Internet Censorship in Australia—A 'Clean-Feed'?*, (July 2009), http://www.mannkal.org/downloads/scholars/internet-censorship-in-australia.pdf; *see also* Bambauer, *supra* note 51, at 494.

69. *See generally* MICHAEL CHESTERMAN, FREEDOM OF SPEECH IN AUSTRALIAN LAW: A DELICATE PLANT 75 (2000).

70. Arthur, *supra* note 66.

71. *Id.*

72. *Id.*

> some limits, like child pornography, are obvious. No Australian wants that to be available and we agree . . . [b]ut moving to a mandatory ISP-level filtering regime with a scope that goes well beyond such material is heavy-handed and can raise genuine questions about restrictions on access to information.[73]

An already hostile Australian society was further fueled in their opposition to recent censorship proposals[74] when whistleblower website Wikileaks published an alarming list purported to be the current Australian blacklist.[75] The alleged list revealed that roughly 2,300 URLs were contained on the blacklist, and that despite repeated assurances by authorities that the list contained only material directly linked to "child sexual abuse, rape, incest, bestiality, sexual violence and detailed instruction in crime," nearly two thirds of the blacklist was comprised of URLs and material that adults have a legal right to both access and possess.[76]

Following the controversial leak, the Australian Broadcasting Corporation reported that "[a]s well as child pornography, the list . . . also includes online gambling sites, YouTube links, regular porn and fetish sites, and websites of a tour operator, Queensland boarding kennel and a Queensland dentist."[77] Although Australian Parliament and the ACMA have vehemently denied the authenticity of the leaked list,[78] they

---

73. *Id.*

74. A discussion among Australian internet users on HACKER NEWS (thread available at http://news.ycombinator.com/item?id=522706) following the leak of the blacklist included the following comment: "We're hoping the leaking of the list comes as a real blow to the government's 'clean feed' censorship plans. . . . All this censorship nonsense really makes me ashamed to be Australian." Another commenter responded, "After you spend a few more hours being ashamed, get MAD!!! . . . This AU firewall-in-progress is a serious battleground for freedom of speech of all developed nations."); *see also* Dan Walmsley, *It's time to get angry about Australian Internet censorship* (Aug. 17, 2009), http://www.danwalmsley.com/2009/08/27/its-time-to-get-angry-about-australian-internet-censorship/.

75. Oliver Luft, *Wikileaks Taken Offline After Publishing Australia's Banned Websites*, GUARDIAN NEWS & MEDIA LTD. (Mar. 19 2009), http://www.guardian.co.uk/media/pda/2009/mar/19/wikileaks-banned-australian-websites.

76. Bowden, *supra* note 59; Nicolas Suzor et al., *Submission to the Department of Broadband, Communications and the Digital Economy 'Mandatory internet service provider (ISP) filtering: Measures to increase accountability and transparency for Refused Classification material ' consultation*, ELECTRONIC FRONTIERS AUSTRALIA, 5 n.10 (Feb. 2010) http://nic.suzor.net/wp-content/uploads/2010/02/2010-EFA-DBCDE-Transparency.pdf ("As at September 2009, it is clear that only one-third of material that is Refused Classification on the ACMA Blacklist was child sexual abuse material; two-thirds of RC material on the ACMA blacklist is legal to view and possess in Australia.").

77. Nic MacBean, *Internet Filter Blacklist Leaked on Web*, ABC NEWS (Mar. 19, 2009), http://www.abc.net.au/news/stories/2009/03/19/2520591.htm.

78. Suzanne Tindal, *Leaked List Not ACMA Blacklist: Conroy*, ZDNET (Mar. 19, 2009), *available at* http://www.zdnet.com.au/leaked-list-not-acma-blacklist-conroy-339295547.htm.

responded by referring to the controversial leak as "grossly irresponsible" and then proceeded to add the Wikileaks website to their blacklist.[79]

IV. INTERNET CENSORSHIP IN THE UNITED STATES

The First Amendment of the United States Constitution provides that "Congress shall make no law . . . abridging the freedom of speech."[80] This protection of free expression extends to speech in print and online formats.[81] American critics of foreign democracies' censorship policies often overlook this significant disparity between free speech rights of these nations and the United States. Australia, as previously discussed, does not have an express guarantee to the freedom of expression or any equivalent provision to the First Amendment of the U.S. Constitution.[82]

It is this venerable guarantee from the founding fathers and creators of the U.S Constitution that has shielded U.S. citizens from encountering any unwarranted restraints on free speech or expression, including any overreaching equivalent in the cyber realm.[83] The government made two notable attempts to enact Federal laws with the objective of censoring certain categories of online content. However, neither one of these laws are currently in force.[84] In addition, several states within the U.S. have attempted to pass censorship laws, which were also struck down on Constitutional grounds shortly after their conception.[85]

In 1996 the U.S. implemented the Communications Decency Act (CDA),[86] marking the government's first attempt to restrict material deemed inappropriate on the Internet. The CDA was a statute making it a federal crime to transmit material that, "under contemporary community standards, would be deemed patently offensive to minors."[87]

In the months following its enactment, portions of the CDA were restrained, until it was ultimately struck down by the Supreme Court in

79. *Id.*
80. U.S. CONST. amend. I.
81. *See* Reno v. ACLU, 521 U.S. 844 (1997) [hereinafter Reno II].
82. Arthur, *supra* note 66.
83. *See* Aaron D. White, *Crossing the Electronic Border: Free Speech Protection for the International Internet*, 58 DEPAUL. L. REV. 491, 507 (2009).
84. The unsuccessful attempts to implement these laws (the CDA and COPA) are discussed below.
85. *Id.*
86. Communications Decency Act (CDA) of 1996, 47 U.S.C. § 223.
87. ACLU v. Reno, 217 F.3d 162, 166 (3d Cir. 2000) [hereinafter Reno I].

the landmark case *Reno v. American Civil Liberties Union*.[88] The Court held that "the CDA lacks the precision that the First Amendment requires when a statute regulates the content of speech," thereby confirming that the Internet is entitled to the same level of First Amendment protections, and therefore the same level scrutiny in its restrictions as offline media.[89] The Court unanimously voted to strike down the anti-indecency provisions of the CDA as an "unnecessarily broad suppression" that effectively prevented adults from engaging in indecent speech, which has traditionally received significant First Amendment protection.[90]

The Court held that in order to prevent minors from accessing this potentially harmful material, the CDA "suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another."[91] Furthermore, while protecting minors is certainly a compelling interest, the Court held that to place the burden of that protection on adult speech "is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve."[92]

The significance of *Reno v. ACLU* is twofold.[93] First, it provides the initial assurance that the First Amendment protects speech and expression in its various formats, including speech that occurs over the Internet.[94] Second, it provides a general confirmation that the U.S. will continue to treat potential legal disputes and other criminal activity conducted on the Internet by applying the same legal standards and Constitutional guarantees as those afforded to persons and activities conducted offline.[95]

The next notable attempt by the American government to enact a proposal intended to censor objectionable content on the Internet was the adoption of the Child Online Protection Act (COPA) in October 1998.[96] COPA, similar to the CDA, was intended to ensure that children could not access "material harmful to minors" on the Internet.[97] This Act ensured compliance by legally requiring commercial websites to restrict access to their content by minors, but provided an affirmative defense to publishers that made attempts to restrict access through age verification

---

88. *Reno II*, 521 U.S. at 844.
89. *Id.* at 846.
90. *Id.* at 875.
91. *Id.* at 846.
92. *Id.* at 874.
93. *Reno I*, 217 F.3d at 166.
94. Corn-Revere, Robert, *The First Amendment and the electronic media*, FIRST AMENDMENT CTR, *available at* http://www.firstamendmentcenter.org//speech/internet/overview.aspx.
95. *Id.*
96. Child Online Protection Act (COPA) of 1998, 47 U.S.C. § 231.
97. *Reno II*, 521 U.S. at 871.

and credit card requirements.[98] Upholding an initial temporary injunction by a Pennsylvania District Court, the Court of Appeals correctly predicted "due to technological limitations, COPA—Congress' laudatory attempt to achieve its compelling objective of protecting minors from harmful material on the World Wide Web—is more likely than not to be found unconstitutional as overbroad on the merits."[99]

Advocates of filtering the web allege that the problem with the U.S.'s approach to censorship, as demonstrated in these two cases, is within the guarantees of the Constitution and those who maintain "radical" views on the protection it affords.[100] They contend that the groups fighting to preserve these freedoms are simultaneously blocking the implementation of policies that are only intended to protect children and aid in the censorship that is necessary to effectively do so.[101] Alternatively, opponents contend that if certain Constitutional "exceptions" are permitted to serve as a safeguard to vulnerable groups, while there are other less restrictive means available, the door is then open for further intrusions by the government.[102]

These two holdings "breathed new life into disputes about what kind of speech may be excluded from First Amendment protection" and their "connection to this new medium confirms that technological change will continue to fuel debates over the meaning and scope of the First Amendment."[103]

V. INTERNET CENSORSHIP IN THE U.K.

In 1996, the Internet Watch Foundation (IWF)[104] was formed in the United Kingdom in response to police investigations that revealed ISPs were inadvertently carrying indecent newsgroup content containing obscene images to the public.[105] The objectionable images hosted by ISPs included those depicting the sexual abuse of children, which were in direct violation

98. *Id.* at 860–61.
99. *Reno I*, 217 F.3d at 181.
100. Donna Rice Hughes, *Filters Don't Censor, They Protect Our Kids: Foes of Internet filter law don't understand the dangers of online porn*, PROTECTKIDS.COM (Mar. 27, 2001), http://www.protectkids.com/donnaricehughes/article_filtersdontcensor.htm.
101. *Id.*
102. *Reno II*, 521 U.S. at 879.
103. Corn-Revere, *supra* note 94.
104. *IWF History*, INTERNET WATCH FOUND., http://www.iwf.org.uk/about-iwf/ iwf-history [hereinafter IWF] (last visited Sept. 2, 2011).
105. *Id.*

of the Protection of Children Act of 1978.[106] The IWF was formed with the purpose of reviewing and responding to reports from U.K. citizens of potentially illegal content discovered on the Internet. The organization was established "to fulfil [sic] an independent role in receiving, assessing and tracing public complaints about child sexual abuse content on the internet and to support the development of website rating systems."[107]

Unlike the ACMA, created to facilitate the censorship of objectionable online content in Australia,[108] the IWF does not initiate independent investigations, but rather assesses potentially objectionable content only in response to reports made by the public.[109] The IWF is a non-governmental, charitable body that reviews these citizen reports and formulates a "black list" comprised of all the websites that host unsuitable information that is, or is believed to be, in contravention to U.K. laws.[110] It is the offline laws in the U.K. that govern what is suitable online; there is no separate classification or standard for what is considered inappropriate or illegal in the online realm.[111]

U.K. censorship policies focus primarily on combating the spread of obscene material that depicts the sexual abuse of children.[112] Although the blocked list compiled by the IWF is not publically available, the organization maintains that "[e]very URL on the list depicts indecent images of children, advertisements for or links to such content."[113] The nature of the material in question is assessed in accordance with U.K. law, and if ultimately added to the block list, is done so on the belief that it is criminal.[114] The criminality of this material is embodied in the Sexual Offenses Act of 2003, which contains criteria established by the U.K. Sentencing Guidelines Council.[115] These guidelines are comprised of assessment levels that are applied to determine the sexually offensive and criminal nature of both offline and online material in the U.K.[116]

---

106. EFA, *supra* note 14.
107. IWF, *supra* note 104.
108. EFA, *supra* note 54.
109. RONALD DEIBERT ET AL., ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 188 (MIT Press 2008).
110. Weixiao Wei, *Online Child Sexual Abuse Content: The Development of a Comprehensive, Transferable International Internet Notice and Takedown System*, http://www.iwf.org.uk/assets/media/resources/IWF%20Research%20Report_%20Development%20of%20an%20international%20internet%20notice%20and%20takedown%20system.pdf.
111. *Remit, Vision and Mission*, INTERNET WATCH FOUND., http://www.iwf.org.uk/about-iwf/remit-vision-and-mission (last visited Sept. 2, 2011).
112. *IWF Facilitation of the Blocking Initiative*, INTERNET WATCH FOUND., http://www.iwf.org.uk/services/blocking (last visited Sept. 4, 2011).
113. *Id.*
114. *Id.*
115. Sexual Offenses Act (SOA), (2003) §§ 1–79, 12(3) HALS. STAT. (4th ed.) 746.
116. Wei, *supra* note 110.

While the IWF plays a crucial role in facilitating Internet censorship in the U.K., the organization asserts that their role is "restricted to the compilation and provision list: the blocking solution is entirely a matter for the company deploying the list."[117] The black list, updated twice daily by the IWF, is transferred to ISPs which are then encouraged to abide by the restriction of the sites contained therein. If an ISP chooses not to follow the IWF's recommendations, it risks ineligibility to contract with the government and other adhering public bodies.[118] Exploring the mechanisms employed by the U.K. government in order to ensure compliance by ISPs in these filtering efforts, the U.K.'s *Times Newspaper* explains:

> The ban on public bodies signing contracts with companies that do not actively block paedophile sites was announced by the Office of Government Commerce.
>
> In an instruction to all departments, agencies and quangos, it said that they should deal only with contractors who agreed to block a list of sites known to carry abusive images. The list, containing between 500 and 800 websites, is maintained by the Internet Watch Foundation and updated twice daily.
>
> An "action note" issued to all departments said the new policy applied to contracts with internet firms, mobile operators, search providers and filtering companies. The note said: "The Government should lead by example and require its suppliers of internet services to deploy the list across services they provide to Government."[119]

Despite the obvious business incentives for domestic ISPs to abide by the filtering regulations distributed by the IWF, to date, there is no legally mandated censorship law in effect in the U.K.[120] Aside from this "informal pressure" placed on ISPs to abide,[121] servers are free to open search results to the materials blacklisted by the IWF. However, reports show that approximately 98% of all Internet users in the U.K. are blocked from access to the materials placed on the black lists.[122] This is an indication that most, if not all, ISPs have chosen to comply.

---

117. IWF, *supra* note 104.
118. *Id.*
119. Sean O'Neill, *Government Ban on Internet Firms That Do Not Block Child Sex Sites*, TIMES ONLINE (Mar. 2010), http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article7055882.ece.
120. EFA, *supra* note 14.
121. Travaglione, *supra* note 68.
122. Wei, *supra* note 110.

In December 2000, the U.K. government published the "Communications White Paper"[123] which addressed the "new communications environment" and the regulation approaches that would soon be implemented in response.[124] While many feared that this would mark the beginning of a new Internet in the U.K., the White Paper ultimately indicated that regulation of the Internet would be left outside the scope of this new legislation.[125] The government's response to Internet regulation was addressed in chapter 6.10.1, stating:

> The Government sees enormous benefits in promoting new media, especially the Internet. But it is important that there are effective ways of tackling illegal material on the Internet and that users are aware of the tools available, such as rating and filtering systems, that help them control what they and their children will see on the Internet. Research suggests that this is what people want in relation to the Internet, rather than third party regulation.[126]

This publication, and the subsequent adoption of the Communications Act of 2003 made it clear that the government had no discernable intent to enact Internet censorship via legislation.[127]

The U.K.'s current censorship policy, unlike the policies proposed in Australia and those discarded in the U.S., does not involve legislation specific to the Internet.[128] Its approach to the regulation of Internet content involves allowing Internet users "to regulate their own internet experience" by offering tools to assist citizens in controlling the content that they see, rather than giving this power to a third party or requiring compliance by law.[129]

The U.K. government has, however, taken an active role in the construction of this rating and filtering system, as well as in the operation of the IWF.[130] It has also informed the public that it supports, and will continue to encourage the work of the IWF by encouraging compliance with these efforts where available.[131] This policy has been effective, although at times slow, with only minimal opposition by citizens of the U.K.[132]

---

123. COMMUNICATIONS WHITE PAPER, *A New Future For Communications* (2003), *available at* http://www.antelope.org.uk/publications/regulation%20and%20internet%20commsbill.pdf.

124. The regulation approaches implemented are embodied in the Communications Acts of 2003. *See* COMMUNICATIONS ACT, 2003, c. 21 (Eng), *available at* http://www.legislation.gov.uk/ukpga/2003/21/pdfs/ukpga_20030021_en.pdf.

125. *Id.*

126. COMMUNICATIONS WHITE PAPER, *supra* note 123, at 13.

127. COMMUNICATIONS ACT, *supra* note 124.

128. EFA, *supra* note 14.

129. *Id.*

130. IWF, *supra* note 104.

131. EFA, *supra* note 14, at 16.

132. *Id.*

These policies have been successful because these methods enable the public to play an active role in determining which content is (at least initially) unsuitable for viewing by their own standards of reasonableness.[133] Although the IWF ultimately makes a determination as to the legality of this content, it does so in accordance with the UK's offline laws. These determinations by the IWF serve more as an additional safeguard than a unilateral determination, because citizens are at least guaranteed that the determinations are made in accordance with offline laws.[134]

VI. RULING OUT GLOBAL CENSORSHIP

Some theorists suggest that an international approach to Internet censorship is the key to a legitimate and effective regulation policy.[135] They argue that reciprocal participation by governments and their respective ISPs is necessary in order to ensure that wholly objectionable and illegal content is effectively removed from within the borders of the nation in which it is hosted.[136] They believe that only this approach will be entirely effective, because only the nation in which this content is hosted has the legal authority to effectuate its removal.[137]

Although in theory this is an attractive option, in execution, it is not a feasible one. Not only do standards of decency vary significantly across borders, but also the objectives of various governments in implementing these censorship policies are vastly dissimilar.[138] Defining indecency on a global scale is a task that would pose vast, if not insurmountable

133. *See supra* note 123 and accompanying text (explaining that the government will to continue to allow citizens to "control what they and their children will see on the Internet" through rating and filtering based on their own standards).

134. The U.K. does not have laws specialized to the online realm; therefore, all determinations must be made in accordance with offline laws. *Id.* ("The United Kingdom has not enacted censorship legislation specific to the Internet and appears to have no intention of so doing.").

135. Elaine M. Chen, *Global Internet Freedom: Can Censorship and Freedom Coexist?*, 13 DEPAUL-LCA J. ART & ENT. L. & POL'Y 229, 232 (2003). ("Internet censorship and jamming protocol should be left to an international arena, such as the United Nations, where a more 'neutral' Internet resolution can be enforced.").

136. ACCESS CONTROLLED: THE SHAPING OF POWER, RIGHTS, AND RULE IN CYBERSPACE 64 (Ronald J. Deibert et al. eds., 2010).

137. *Id.*

138. Bambauer, *supra* note 35, at 384.

difficulties. It only takes brief examination of the current decency standards and government objectives in order to recognize the deficiency.[139]

Standards of decency in democracies structured akin to the U.S. would require a narrowly tailored definition to pass Constitutional muster, which would fail to translate across borders to nations that are not similarly composed. Italy, for example, does not criminalize zoophilia,[140] BDSM,[141] or fetishism,[142] whereas these acts in certain forms are strictly prohibited in the U.S.[143] Australia,[144] and illegal under specialized regulation in the U.K.[145] Germany censors material containing holocaust denials; China actively censors political dissent, and Brazil and Canada censor broad categories of racial hate speech.[146] Furthermore, Australian proposals appear to be aimed at ultimately censoring indecent or "unsuitable" material including graphic pornography, racial hate speech, and extreme violence—much of which is legal to view and possess by adults in most other democratic nations, and is protected by the U.S. Constitution.[147]

Even if it were feasible to construct a definition or standard of indecency that encompassed, without restricting, global interpretations of what should be absolutely eliminated from the cyber realm, this global policy would prove futile for nations seeking stricter levels of censorship. These nations would waste time and resources by participating in a global censorship scheme, as they would ultimately still need to implement their own policies in order to accomplish their more rigorous objectives. Consequently, many nations would have little incentive to

---

139. Green, *infra* note 146 ("Censorship is international, continuous and pervasive, but it is not a seam-less monolith. Concerns that seem paramount to one nation are meaningless to another.").

140. "Zoophilia" is an erotic fixation on animals that may result in sexual excitement through real or fancied contact. MERRIAM-WEBSTER, http://www.merriam-webster.com/medical/zoophilia.

141. The term "BDSM" is an abbreviation derived from the terms bondage and discipline, domination and submission, sadism and masochism. WIKIPEDIA, http://en.wikipedia.org/wiki/BDSM.

142. "Fetishism" is the displacement of sexual arousal or gratification onto a fetish (e.g., onto an alternate object or body part). DICTIONARY.COM, http://dictionary.reference.com/browse/fetishism.

143. Depiction of animal cruelty, 18 U.S.C. § 48, Pt. I, Ch. 3 (2000).

144. HALSBURY'S LAWS OF AUSTRALIA, vol. 9, p. 247662 (Sydney: Butterworths, 1999) (laws implemented by Province).

145. Criminal Justice and Immigration Act, (2008) § 63, 12(4) HALS. STAT. (4th ed.) 649.

146. Jonathon Green & Nicholas J. Karolides, THE ENCYCLOPEDIA OF CENSORSHIP 72, 106, 224–36 (Facts on File. Inc., 2005); Const. of Brazil, 5 Oct. 1988, *available at* http://www.unhcr.org/refworld/docid/4c4820bf2.html.

147. *AU Gov't Mandatory ISP Filtering/Censorship Plan*, LIBERTUS.NET (last modified Aug. 4, 2011), http://libertus.net/censor/isp-blocking/au-govplan.html#s40; ([M]any of the sub-categories of "RC" involve material legal to sell/publish in other

participate in a global system, particularly if the guidelines are tailored to fall within the scope of the U.S. Constitution.[148]

VII. PROPOSAL: ACQUIRING PUBLIC APPROVAL THROUGH LEGITIMACY, TRANSPARENCY AND EFFECTIVENESS

In order for a censorship policy adopted by a democratic nation to be effective, public approval is imperative. The organizations and populations that structure these democratic nations have frequently demonstrated this condition, and the dawn of new media has made it even easier for these groups to act on their frustrations to effectuate change.[149] When the public perceives the government becoming less accountable, and those capable, if not responsible, for preventing these infringements (media outlets, ISPs) becoming less independent from the government, they have, and will continue, to take action and voice their concerns.[150]

In order to acquire public approval, a censorship proposal must: (1) clearly articulate the objectives of the government; (2) reflect the stated objectives; (3) exhibit transparency in order to ensure that the policy reflects the stated objectives; (4) acquire legitimacy through a valid foundation in offline laws; and (5) be effective in accomplishing its intended purpose.

A. Articulate the Objectives of the Government

The first two requirements, that censorship policies clearly articulate and ultimately reflect the stated objectives of the government, are grounded in the Lockean notion that a democratic government is responsible for representing and serving the interests of the people by whom they were elected.[151] The government must therefore ensure that its ultimate goal

148. This Comment dismisses a global standard as the solution to accomplishing the objectives of democratic nations in censoring content to protect internet users *domestically*; however, it is important to note that a global standard or scheme is a significant (and perhaps essential) step in efforts to undermine heavy handed censorship schemes *internationally*. The focus of this Comment is on constructing a workable filtration scheme within democratic nations, not on resolving global censorship issues. Thus, democratic nations would have little incentive to participate in a global scheme aimed at protecting the interests of their own citizens.

149. *See infra* notes 167–68.

150. *Id.*

151. This idea is embodied in John Locke's theory of government based on the consent of the governed. JOHN LOCKE, SECOND TREATISE OF CIVIL GOVERNMENT 238 (The Lawbook Exchange, Ltd. 2006) (1698).

in constructing any regulatory policy is to serve and protect the interests of the people. It is important that the grounds for implementation of any proposed regulation be clearly articulated to the public so that they are able to recognize that their own interests are the ultimate goal of the government's in crafting any policy to regulate Internet content.[152]

B. Reflect the Stated Objectives

It is not enough, however, that the government *articulate* their objectives in order to demonstrate its goal of serving the people. The proposed policy must actually *reflect* the government's stated objectives. The consequences of acting in contravention to stated objectives was observed in Australia's foray into Internet censorship.[153]

As was previously discussed, Australian Parliament developed an Internet content categorization system,[154] which it used as the basis for its censorship policy and black list, and informed the public that it only intended to block sites that fell within the "RC category."[155] After repeated assurances that the objective of the policy was the protection of minors, and that *all* of the material blocked contained prohibited child pornography and abuse, a leak ultimately revealed that broader, protected categories of speech were being censored as well.[156] Whether these incidental blocks were deliberate or attributable to a combination of human and technological error, does not alter the detrimental effect that they had on the level of support for the censorship policy itself.[157]

If the government states that its objective is the protection of minors, it should not regulate any content that falls outside the scope of this objective. The failure to act in accordance with stated objectives creates political distrust—democracy's greatest adversary in attempting to accrue support for the implementation of unfamiliar and unfavorable policies. Any discernable contradiction between the stated objectives and the actions of the government may not only result in an immense decrease in support

---

152. For example, the protection of their children being the objective of implementing a policy to censor certain types of pornography.

153. Luft, *supra* note 75.

154. *See supra* notes 50, 51.

155. *Id.*

156. Suzor, *supra* note 76; Belinda Luscombe, *A Blacklist for Websites Backfires in Australia*, TIME (Mar. 27, 2009), http://www.time.com/time/business/article/0,8599,1888011,00.html.

157. Richard Phillips, *Australian Photographer Bill Henson—scapegoat for a wider assault on democratic rights*, WORLD SOCIALIST WEB SITE (May 30, 2008), http://www.wsws.org/articles/2008/may2008/hens-m30.shtml.

for presently proposed regulation policies,[158] but is also likely to impede confidence in future policies, despite potential legitimacy.

C. Transparency

In order to assure the public that proposals to censor content on the Internet veritably reflect stated governmental objectives, governments must offer a level of transparency in both their policies and the URLs that are ultimately censored or placed on blacklists.[159] This is perhaps the most contentious matter in current legislative attempts to acquire support for censorship proposals.

Both Australian and British citizens have petitioned for transparency in the lists compiled for regulation, but governments have been unwilling to comply.[160] Frank Fisher, a critic of the UK's failure to offer transparency, expressed the complaint in this way: "[t]his is, remember, that same government that's constantly telling us, with regard to ID cards, that if you have nothing to hide, you have nothing to fear. Why then, do they hide this list?"[161]

In response to more pressing calls for transparency by an apprehensive Australian population, the Minister for Broadband, Communications and the Digital Economy, Senator Stephen Conroy, issued a press release. Conroy articulated Parliament's (and the ACMA's) reasoning for repudiating a transparent policy stating, "the problem when you produce a list of URLs is you are actually giving the address of where to go and look."[162] Critics challenge this as an unfounded excuse, posing the obvious argument that if the proposed filtering policy is going to be effective, these sites should not be accessible regardless of people knowing where to look.[163] So either "the filter will block websites Australian's aren't meant to be accessing, in which case it really doesn't

158. Asher Moses, *'Caching error' caused Henson blacklisting*, THE SYDNEY MORNING HERALD (Mar. 27, 2009, 2:54 PM), http://www.smh.com.au/articles/2009/03/27/1237657133829.html.

159. *Id.*

160. Media Release, National Broadband Network, Outcome of Consultations on Transparency and Accountability for ISP Filtering of RC Content, (July 9, 2010), (*available at* http://www.minister.dbcde.gov.au/media/media_releases/2010/068).

161. Fisher, *supra* note 18.

162. Oz, *Stephen Conroy admits internet filter is useless*, OZSOAPBOX (Mar. 30, 2010), http://ozsoapbox.com/rest-of-australia/censorship/stephen-conroy-admits-internet-filter-is-useless.

163. *Id.*

matter if the banned URL list is made public or not, or the filter won't work."[164] Furthermore, if the policy conforms to the stated objectives of the government in primarily blocking child pornography, few people should feel compelled to circumvent the system in order to access the banned material, unless of course, they want to risk facing criminal penalties.[165]

If democratic governments continue to seek filtration via blacklists that lack transparency, they are not only depriving citizens of the participation they are entitled to, but are offering control to third party operators who have only *implied* accountability to the public. Without transparency, the incentives, accuracy, and effectiveness of third party operators will remain cynical in the eyes of the public. Although a disinterested third party operator may be more reliable in performing this task than the government itself, without transparency, no organization responsible for compiling the list will attain widespread legitimacy. The adoption of a transparent policy would not only serve to generate support for regulation that current policies lack, but it would increase attention and oversight by these third party operators for fear of making a mistake. In addition, transparency would enable public oversight that would quickly and appropriately help to identify and eliminate any errors overlooked by the operators. Transparency would ensure that the government has confidence in its system, and the people have confidence in its methods.[166]

Governments need to recognize—as ISPs refusing "heavy handed" censorship have—that the Internet is a global "median that pays no attention to borders, and . . . militates against control."[167] Where governments fail to hear calls for transparent reform, other entities will, and they will respond accordingly through measures that offer the transparency sought by

---

164. *Id.*

165. For example, facing criminal penalties for contravening well-established offline laws against possessing and distributing child pornography. *See* SOA, *supra* note 115.

166. Some jurisdictions have already experimented with and adopted transparent censorship policies. For example, in Saudi Arabia:

> [U]sers are presented with a blockpage which states that the requested Web site has been blocked but it also contains a link to a Web form through which users can petition to have the site unblocked . . . . The acknowledgement of blocked content allows users to petition to have sites unblocked if there has been a mis-classification. It also requires governments to justify why a specific site is blocked.

Nart Villeneuve, *The Filtering Matrix: Integrated Mechanisms of Information Control and the Demarcation of Borders in Cyberspace*, FIRST MONDAY (2006) 11(1), *available at* http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1307/1227.

167. Boorstin, *infra* note 168; *see also* Rosa Golijan, *Google Refuses to Continue Censoring Results in China*, GIZMODO (Jan. 12, 2010, 6:25 PM), http://gizmodo.com/5446712/google-refuses-to-continue-censoring-results-in-china.

dissatisfied citizens.[168] Nontransparent policies will ultimately result in cyber protests through hacks,[169] leaks,[170] and the assembly of organizations such as Wikileaks,[171] with the goal of bringing frustrations to the attention of the general public. As articulated by Wikileaks on the organization's webpage:

> Publishing improves transparency, and this transparency creates a better society for all people. Better scrutiny leads to reduced corruption and stronger democracies in all society's institutions, including government, corporations and other organisations. A healthy, vibrant and inquisitive journalistic media plays a vital role in achieving these goals. We are part of that media.[172]

D. Legitimacy Through a Foundation in Offline Laws

If democratic nations want to implement policies that will not be met with opposition by their respective populations, they also need to ensure the laws they implement online obtain legitimacy by reflecting the rights granted to their citizens offline. Governments cannot and should not use the Internet as a means of covertly eliminating unfavorable content that is not regulated by offline laws. Implementing an online censorship scheme that has no legal basis offline is not a policy that will endure in a Western democracy, and is not a policy that will or should gain support from the organizations and bodies involved in its implementation.

Inherent in the democratic freedom of speech is the right to converse without censorship or restraint. This freedom of expression empowers

---

168. Robert Boorstin, Google Director of Corporate and Policy Communications, Address at the Geneva Summit for Human Rights Tolerance and Democracy (Mar. 9, 2010*) (available at* http://blog.unwatch.org/index.php/2010/04/29/google-internet-censorship-getting-worse-more-sophisticated/) (excerpt from Boorstin's speech).

> Just yesterday . . . the United States Treasury Department lifted what has been a long-time ban on allowing companies like ours to license certain kinds of software . . . to countries like Iran and Sudan. [T]his is a great accomplishment. We feel it's something the companies and human rights groups argued for together.

Id.

169. Kathy Marks, *"Operation 'Titstorm" Hackers Declare Cyber War on Australia*, THE INDEPENDENT (Feb. 11, 2010), http://www.independent.co.uk/news/world/australasia/operation-titstorm-hackers-declare-cyber-war-on-australia-1895838.html (discussing action taken by anonymous hackers following announcements regarding implementation of internet restrictions in Australia).

170. Luft, *supra* note 75.

171. About Wikileaks, *1.3 Why the Media (and Particularly Wikileaks) is Important*, WIKILEAKS, http://wikileaks.org/About.html (last visited Sept. 5, 2011).

172. *Id.*

members of democratic societies to communicate and access information without censorship over the content of their ideas. Despite this fundamental canon of democracy, the freedom of expression is not absolute.[173] Democratic administrations have traditionally recognized that the need to prevent certain illicit activities outweighs the need protect peoples' right to encourage and engage in them.[174]

E. Effective in Accomplishing Stated Objectives

The final requirement for any form of Internet regulation to gain support and favorable understanding in a western democracy is the policy effectively does what it is implemented to do.[175] In addition, if an equally effective policy could be implemented in a less restrictive manner, the alternate mechanism should be fully explored prior to the implementation of a censorship scheme.[176] Ensuring effectiveness can be accomplished by weighing the interests of regulating the appropriate content versus swift implementation, and recognizing that speed should be sacrificed for increased effectiveness. Ultimately, ensuring that proper designations and removals are being made is more important than a swift and strong solution, which would likely be accompanied by inaccuracies and subsequent corrections.

For example, Australia's ACMA blacklist contained contemporary art photographer Bill Henson's website, despite its mere PG classification. Although there were other misclassifications,[177] this was the only "PG" classification[178] that earned itself a spot on the blacklist. Notably, this was not Henson's first confrontation with Australian authorities over the notorious content of his work.[179] When confronted about the blacklisting of such innocuously rated[180] material, Australian Senator Stephen Conroy

---

173. *See generally When Can't I Say That?*, EDUCATION FOR FREEDOM, http://www.freedomforum.org/packages/first/Curricula/EducationforFreedom/L04main.htm (last visited Aug. 26, 2011).

174. Commonly subject to limitations are things such as hate speech and the incitement of imminent lawless action. *Id.*; Brown, 45 M.J. at 395 (citing Cohen v. California, 403 U.S. 15, 91 S.Ct. 1780, 29 L.Ed.2d 284 (1971). ("[T]he right to free speech is not absolute, and some speech—e.g., dangerous speech, obscenity, or fighting words—is not protected by the First Amendment, regardless of the . . . status of the speaker.")).

175. *See generally* Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557 (1980).

176. *See generally* Ashcroft v. ACLU, 542 U.S. 656 (2004).

177. MacBean, *supra* note 77.

178. NATIONAL CLASSIFICATION CODE, *supra* note 49.

179. Phillips, *supra* note 157.

180. Henson's website was innocuously rated, but was not necessarily "innocuous" content. Henson had previously been accused of using underage models in his work. The problem, however, is that the government failed to abide by its own rating system.

divulged that the blacklisting of Henson's URL was an oversight attributed to "a caching error in the system."[181] He also assured the public this was the only mishap of its kind.[182] Critics often cite this incident as grounds necessitating transparency.[183] Regardless of who is responsible for the improper censorship, the oversight could have been swiftly resolved, or prevented entirely by a transparent system.

VIII. INFRASTRUCTURE: A FOUNDATION OF COOPERATION AND ACCOUNTABILITY

As this Comment has explored, while democracies share similar legislative doctrines, they maintain numerous dissimilarities in composition and community standards. It is, therefore, impractical to pose an infrastructure for censorship that would be workable across borders. There are, however, some key attributes that all democratic administrations should take into consideration when designating the infrastructure of their Internet regulatory policies.

A. Public Participation

First, the public should have the ability to report websites they believe to contain material that would be determined unsuitable. This requires that there be public access to the applicable standards, discussed further in the "Publication Section" below. Some level of public participation is integral to a successful regulation scheme, although the manner in which people file their complaints may fluctuate. This participation should not constitute a final determination, but should serve as a mechanism that enables citizens to report websites that may have been overlooked by the responsible reviewing entity. There is no doubt that there are more Internet users than there will ever be Internet regulators. Therefore, it is both appropriate and efficient to enable users to participate in the infrastructure of their own regulation policy if they come across content that may be inappropriately accessible.

This essentially indicates that without transparency, the government could make arbitrary blocking decisions contrary to assurances made to the public. Furthermore, this was not the only misclassification that caused alarm. *See* MacBean, *supra* note 77.

181. Moses, *supra* note 158.
182. *Id.*
183. *Id.*

It is important, at this stage, to involve the public and enable them to report material that may have been overlooked. Public participation contributes to public approval of a policy and has the potential to increase effectiveness; however, it should not impact the final determinations, other than by bringing potential violations to the attention of the reviewing entity.

B. Reviewing Entity

The reviewing entity is the party responsible for formulating the blacklist by reviewing citizen reports, conducting independent investigations, and applying the law to the websites in question. This body should be akin to the ACMA in Australia or the IWF in the U.K. They are also responsible for forwarding the blacklist of sites, determined to be in contravention of the nation's laws, to ISPs.

While it appears that more success and support has been generated for the British policy of a reviewing entity that is *not* entitled to conduct independent investigations, this may not be a condition that all nations should choose to follow. To ensure that a regulatory scheme is effective, it may not be sufficient to entrust the public with the sole responsibility of finding and reporting illegal and unsuitable content online.

Regardless of whether this entity is entitled to conduct independent investigations, it is imperative that there be a reviewing body or appeals system. This is particularly important in nations such as Australia, which appear to have no plans to adopt a level of transparency in their blacklist compilations.[184] Content publishers that are censored or blocked must have some means of appealing a decision they believe to have been made unfairly or in error.

Nations are likely to delegate the task of reviewing, applying offline laws, as well as the appeals process, to different organizations based on who they believe to be most capable. It is important that regardless of the organization or group formed to handle this task, that the group be "disinterested." They should not have obligations to any other group that may impact or unfairly bias their decision making process. Their job is to apply the law, apply the standards developed, and make a determination based on those facts alone.

C. ISP Cooperation

The interactions between the organizations responsible for formulating blacklists and the ISPs ultimately responsible implementing them, have

184. Media Release, *supra* note 160.

become increasingly complex. Some nations, such as Australia, have attempted to mandate regulation legislatively, while other nations, such as the U.K., have placed informal public and fiscal pressure on ISPs to comply.[185] The U.S. has avoided mandating censorship legislatively, but a recently proposed bill, the Combating Online Infringement and Counterfeits Act (COICA),[186] may drastically change the formerly composed atmosphere. This bill represents a hybrid of the proposed Australian and current British methods, which would mandate ISPs to block certain materials that directly violate offline copyright laws, and place pressure on ISPs to abide by a second set of blacklisted materials "dedicated to infringing activities."[187]

The complications that arise in deciding whether to mandate compliance or encourage cooperation of ISPs have been observed in all three of the nations discussed in this comment. While no obvious solution exists, one thing is absolutely clear: The scope of these regulations may not exceed governmental authority. If there is a clear basis in offline laws then legislative enactments are within the purview of governmental authority. However, where the regulation does not have a clear and convincing foundation in offline laws, democratic administrations cannot mandate the compliance of ISPs. This is important not only to acquire legitimacy at home, but also to ensure that domestic censorship methods do not undermine global democratic endeavors to eliminate unjust censorship policies implemented by repressive regimes abroad.

D. Publication

The body responsible for enabling transparency in a regulation scheme is the government. ISPs complying with past censorship policies abroad have been prohibited from publishing the list of websites placed on the blacklist.[188] Similarly, independent organizations and individuals that have come into possession of these lists have been threatened that publication would result in criminal penalties.[189]

185. Dudley-Nicholson, *supra* note 17; Fisher, *supra* note 18.
186. S. 3804, 111th Cong. § 1 (2010); *see also The COICA Internet Censorship and Copyright Bill*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/coica (last visited Sept. 6, 2011).
187. S. 3804, *supra* note 186.
188. Luft, *supra* note 75.
189. *Id. See also* Luscombe, *supra* note 156.

However, publication is important because without transparency there is an absence of trust, and thus an absence of compliance and any prospect for success. Julian Assange, the founder of Wikileaks, has justified his organization's involvement in similar disclosures against the interests of the government by saying, "our goal is justice our method is transparency."[190] In order to prevent individuals and organizations from seeking justice through unauthorized publication, the government must accept that permitting transparency is a crucial element of a successful Internet regulation policy. In response to Conroy's argument that publication would lead people to seek access to the banned websites, so long as the publication contains enough information for individuals to identify a legitimate basis for censorship,[191] they have no reason to attempt to access the URLs themselves, which they should be unable to do anyway.[192]

IX. CONCLUSION

Meeting the requirements necessary to effectively implement an Internet regulatory scheme in a democratic society hinges on acquiring public approval. As U.S. President Barack Obama stated, "[t]he more freely information flows, the stronger the society becomes, because then citizens of countries around the world can hold their own governments accountable."[193] Acquiring the approval of a public that is freely encouraged to rebuke policies that contravene their rights as citizens must begin with not just ensuring, but *demonstrating* the legitimacy, transparency, and effectiveness of any such scheme.

There are very few who would argue that heinous crimes such as the possession and distribution of child pornography should be legal; however, there are many who would fight against the implementation of policies aimed at censoring such content, in order to protect constitutional rights that may be residually infringed.[194] Consequently, it is up to democratic governments and their citizens to work together to strike a

190. Interview by Hans Lysglimt with Julian Assange, Wikileaks Founder (July 30, 2010), *available at* http://www.lewrockwell.com/orig11/assange2.1.1.html.

191. For example, the approach taken in Saudi Arabia, which requires governments to identify why each specific site is blocked on the blockpage. *See* Villeneuve, *supra* note 166.

192. In other words, if the filtering system is effective, the "blocked sites" should be just that, *blocked.*

193. *Obama Pushes China to Stop Censoring the Internet*, NPR (Nov. 16, 2009), http://www.npr.org/templates/story/story.php?storyId=120450377 (quoting President Obama in speech to Shanghai students).

194. Corn-Revere, *supra* note 94.

balance between the most basic and necessary levels of censorship and the inherently democratic rights of citizens.

Citizens and organizations fighting against regulation, and governments seeking to protect their citizens through regulation, must come together and recognize their common objectives in order to effectuate the changes they wish to see through mutual sacrifice. Citizens must accept that a minimum level of Internet filtration may be necessary for the government to effectively perform the task of preventing and punishing illegal activities conducted online. Similarly, the government must recognize the need for citizens to be both active participants and supporters of any such policy. Consequently, for a censorship scheme to succeed in a democratic nation, it must withstand criticism and accountability, acquire a sufficient level of support and approval, maintain legitimacy through transparency and a valid foundation in offline laws, and effectively accomplish its proclaimed goals.