Fordham International Law Journal

Volume 38, *Issue* 3 2015 *Article* 5

Bringing in a New Scale: Proposing a Global Metric of Internet Censorship

Philip Chwee*

*Fordham University School of Law

Bringing in a New Scale: Proposing a Global Metric of Internet Censorship

Philip Chwee

Abstract

Part I of this Note provides an overview of Internet censorship and international law, including the different approaches and theories behind Internet censorship. Part I.A discusses the development of the ICCPR and its application to the Internet. Next, Part I.B-D provides an in-depth overview of the Internet censorship models of three different countries: the United States, the United Kingdom, and China. Part II examines each country's Internet censorship model under Article 19 of the ICCPR, considering Article 19(3)'s three-part test and requirements established by recent UN reports interpreting them. The analysis will also examine each country's copyright laws under Article 19. In Part III, this Note argues that due to the idiosyncrasies of each country's Internet censorship policy and new challenges presented by intellectual property laws, Article 19 of the ICCPR by itself does not provide a clear analysis of a country's Internet policy. Article 19 should be supplemented with parts of Professor Bambauer's framework. The culturally-neutral criterion of the framework mitigates the difficulty of analyzing and comparing countries with different cultural norms and moral values. Moreover, the proposed metric also allows for analysis of indirect chilling effects caused by intellectual property laws. This Note concludes that supplementing Article 19 with the framework proposed by Professor Bambauer is a positive step towards creating a global standard of Internet regulation.

KEYWORDS: International Law, Internet Censorship, ICCPR, Artcile 19, Internet policy, United Nations

NOTE

BRINGING IN A NEW SCALE: PROPOSING A GLOBAL METRIC OF INTERNET CENSORSHIP

Philip Chwee[*]

[*] J.D. Candidate, 2015, Fordham University School of Law. The Author would like to thank Professor Olivier Sylvain for his encouragement and advice throughout the drafting process and Sharon Hang and the *Fordham International Law Journal* editors and staff for their help and support.

INTRODUCTION

Every day, a courier begins his route and enters a busy and seemingly endless highway. As he drives, he observes different passing exits. Some exits are patrolled by watchdogs, while towers and formidable walls loom over others. As he enters different exits, he is stopped and examined by each post differently. Some let him pass through freely, some cautiously examine him, and others turn him around without any explanation. This occurs billions of times a day. This is the Internet.

Few if any developments in information technology have had such an effect on society as the creation of the Internet.[1] Moreover, the advent of Internet social media in particular has provided users with an unprecedented level of communication.[2] The expansive reach of social media has played a key role, for example, in coordinating mass protests and keeping the international community informed about situations where journalists have limited access.[3] Recognizing

1 *See, e.g.*, Mike Lata, *How the Internet Revolutionized Human Interactivity*, EXAMINER (Dec. 12, 2011), http://www.examiner.com/article/how-the-Internet-revolutionized-human-interactivity (describing the Internet's influence on human interaction); Courtney Myers, *How the Internet is Revolutionizing Education*, THE NEXT WEB (May 14, 2011), http://thenextweb.com/insider/2011/05/14/how-the-Internet-is-revolutionizing-education/ (describing how the Internet has shifted education paradigms).

2. *See* Karan Chopra, *The Effects of Social Media on How We Speak and Write*, SOCIAL MEDIA TODAY (Sept. 17, 2103), http://socialmediatoday.com/karenn1617/1745751/effects-social-media-how-we-speak-and-write (describing how the Internet has not only shaped the way people communicate, but has also transformed our concept of communicating); Lata, *supra* note 1 (noting that the unprecedented, global reach of the Internet has spurred government intervention).

3. *See, e.g.*, Mercedes Bunz, *In Haiti Earthquake Coverage, Social Media Gives Victim a Voice*, THE GUARDIAN (Jan. 14, 2010), http://www.theguardian.com/media/pda/2010/jan/14/socialnetworking-haiti (discussing how social media has played a pivotal role in news reporting during periods of traditional media blackouts); Sam Gustin, *Social Media Sparked, Accelerated Egypt's Revolutionary Fire*, WIRED (Feb. 11, 2011), http://www.wired.com/2011/

the significance of the Internet as an avenue for expression, scholars and UN specialists posit that Article 19 of the International Covenant on Civil and Political Rights ("ICCPR") implies a right to Internet access.[4] The ICCPR is a multilateral treaty that commits its State party members to respect specific civil and political rights of individuals.[5] Article 19 of the ICCPR ("Article 19") establishes a qualified right to freedom of expression.[6] However, the expansion of this sixty-year-old international treaty to the Internet comes with certain difficulties.[7]

The border-defying aspects of the Internet raise an international governance problem on a global scale.[8] Countries are exercising increased control over internal Internet activity, specifically through the use of censorship.[9] Censorship occurs when a government body directly or indirectly prevents communication between a willing speaker and a willing listener through regulations or control.[10] Moreover, governments justify their restrictions based on a variety of norms.[11] For example, China justifies its extensive Internet restrictions for the purposes of maintaining social stability and

---

02/egypts-revolutionary-fire/ (reporting social media's significant influence on the Egyptian Revolution of 2011).

4. *See infra* Part I.A.1 (discussing scholars' interpretations of Article 19 to imply a right to Internet access).

5. International Covenant on Civil and Political Rights, Dec. 19, 1966, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976) [hereinafter ICCPR].

6. ICCPR, *supra* note 5, art. 19.

7. *See infra* Part II (examining the selected country's model of Internet governance under Article 19); *infra* Part III (arguing that Article 19 is insufficient to deal with the current systems of Internet censorship).

8. *See infra* Part I.B-D (describing several countries' different Internet censorship models).

9. *See infra* Part I.B-D (discussing attempts of government regulations of the Internet in selected countries).

10. For the purposes of this Note, censorship also includes government regulations that create indirect chilling effects. In his article, *Orwell's Armchair*, Professor Derek E. Bambauer defines censorship as government interdiction that prevents communication between a willing speaker and a willing listener. *See* Derek E. Bambauer, *Orwell's Armchair*, 79 U. CHI. L. REV. 863, 871 (2012) [hereinafter Bambauer, *Orwell's Armchair*]. However, this definition is too narrow. Prior restraints or prospects of subsequent punishment can also regulate citizens' behavior. *See generally*, William T. Mayton, *Toward a Theory of First Amendment Process: Injunctions of Speech, Subsequent Punishment, and the Costs of the Prior Restraint Doctrine*, 67 CORNELL L. REV. 245 (1982) (discussing how prior restraint and subsequent punishment also suppress speech).

11. *See infra* Part I.B-D (explaining different countries' justification for their Internet censorship).

national security.[12] The United States, on the other hand, permits much more content because the First Amendment provides constitutional protections for free speech.[13]

Additionally, the current system of digital copyright laws adopted by many countries, such as the Digital Millennium Copyright Act and E-Commerce Directive, presents potential complications under the rights guaranteed by Article 19.[14] As a consequence, the combination of the limited text of Article 19 of the ICCPR, the range of censorship and idiosyncratic Internet regulations and intellectual property laws, and the divergence in transnational norms makes it difficult to analyze the legitimacy of a specific country's Internet censorship policy.[15]

Further, countries have employed different methods of protecting copyrights in the digital world.[16] Scholars have criticized certain national copyright laws, specifically intermediary liability and notice-and-action systems, for their potential chilling effect on speech.[17] In response, advocacy organizations, such as the UK-based ARTICLE 19, have recommended changes to the current paradigm of notice-and-action systems in order to limit collateral negative effects.[18]

With visions of creating a uniformly regulated Internet, some theorists argue for an international approach to Internet regulation.[19]

---

12. *See infra* Part I.D (discussing the People's Republic of China's ("PRC's") Internet censorship model).

13. *See infra* Part I.B (describing the US Constitution and its Internet censorship model).

14. *See infra* Part I.B-C (discussing the Digital Millennium Copyright Act ("DMCA") and E-Commerce Directive's impact on internet speech).

15. *See infra* Part III (arguing that Article 19 does not effectively address the various novel issues presented by the Internet).

16. *See infra* Part I.B-D (discussing various countries' approaches to protecting digital copyrights).

17. Governments impose intermediary liability by making communication intermediaries, such as content providers (e.g., YouTube), legally liable for the actions of its users. Notice-and-action is a process, generally established by a statute or court order, of removing content after receiving certain notice. *See Internet Intermediaries: Dilemma of Liability*, ARTICLE 19, http://www.article19.org/data/files/Intermediaries_ENGLISH.pdf (2013) [hereinafter *Internet Intermediaries*] (advocating for a change to the current notice-and-action regimes); *see also Unintended Consequences: Fifteen Years Under the DMCA*, ELECTRONIC FRONTIER FOUND. (Mar. 2013), https://www.eff.org/pages/unintended-consequences-fifteen-years-under-dmca (discussing the DMCA's effect on Internet speech).

18. *See Internet Intermediaries, supra* note 17 (recommending improvements on the notice-and-action systems).

19. *See, e.g.*, Elaine M. Chen, *Global Internet Freedom: Can Censorship and Freedom Coexist?*, 13 DEPAUL-LCA J. ART & ENT. L. & POL'Y 229, 232 (2003) (arguing that Internet

Others argue that, while a global uniform censorship policy is attractive, it is not viable.[20] In an attempt to address the deficiency in current theoretical approaches to Internet governance, Professor Derek E. Bambauer presented a process-based metric for analyzing Internet regulatory systems.[21] The metric examines the openness, transparency, narrowness, and accountability of a country's censorship scheme.[22] While Professor Bambauer developed the metric to be used in analyzing countries' censorship systems, he did not address its potential application to Article 19.[23] This Note argues for supplementing a similar normative metric to Article 19 of the ICCPR. Such a metric would provide clearer guidelines for analyzing the legitimacy of national censorship laws as measured against the potential indirect chilling effects caused by such laws.

Part I of this Note provides an overview of Internet censorship and international law, including the different approaches and theories behind Internet censorship. Part I.A discusses the development of the ICCPR and its application to the Internet. Next, Part I.B-D provides an in-depth overview of the Internet censorship models of three different countries: the United States, the United Kingdom, and China.

Part II examines each country's Internet censorship model under Article 19 of the ICCPR, considering Article 19(3)'s three-part test and requirements established by recent UN reports interpreting them.

---

censorship should be left to an international arena, such as the United Nations); Nart Villeneuve, *Barriers to Cooperation: An Analysis of the Origins of International Efforts to Protect Children Online*, *in* ACCESS CONTROLLED: THE SHAPING OF POWER, RIGHTS, AND RULE IN CYBERSPACE 55, 63-66 (Ronald J. Deibert et al. eds., 2010) (arguing for reciprocal participation of governments and ISPs to remove illegal content).

20. *See, e.g.*, Renee Keen, *Untangling the Web: Exploring Internet Regulation Schemes in Western Democracies,* 13 SAN DIEGO INT'L L.J. 351, 369-70 (arguing that an international approach is not feasible because of the divergence of obscenity standards).

21. Professor Derek E. Bambauer is a Professor of Law at University of Arizona, James E. Rogers College of Law. *See* Derek E. Bambauer, *Cybersieves*, 59 DUKE L.J. 377 (2009) [hereinafter Bambauer, *Cybersieves*] (presenting a process-based metric of openness, transparency, narrowness and accountability for analyzing a country's Internet regulatory scheme).

22. *See* Bambauer, *Cybersieves*, *supra* note 21, at 390 (presenting the framework); *see also* Bambauer, *Orwell's Armchair*, *supra* note 10, at 900-06 (utilizing the framework to analyze attempts of soft-censorship in the United States).

23. *See* Bambauer, *Cybersieves*, *supra* note 21, at 410-18 (arguing for various forms of implementing the framework, but not considering the Human Rights Commission as a viable option or the framework's relevance to Article 19 of the ICCPR).

The analysis will also examine each *country's* copyright laws under Article 19.

In Part III, this Note argues that due to the idiosyncrasies of each country's Internet censorship policy and new challenges presented by intellectual property laws, Article 19 of the ICCPR by itself does not provide a clear analysis of a country's Internet policy. Article 19 should be supplemented with parts of Professor Bambauer's framework.[24] The culturally-neutral criterion of the framework mitigates the difficulty of analyzing and comparing countries with different cultural norms and moral values. Moreover, the proposed metric also allows for analysis of indirect chilling effects caused by intellectual property laws. This Note concludes that supplementing Article 19 with the framework proposed by Professor Bambauer is a positive step towards creating a global standard of Internet regulation.

I. *THE DEVELOPMENT OF INTERNATIONAL HUMAN RIGHTS LAW AND THE INTERNET*

In this Part, Section A will discuss the historical development of the ICCPR and its subsequent application to the Internet. Next, Section B provides an in-depth overview of the Internet censorship models of the United States, the United Kingdom, and China. These countries were selected because each country employs a distinct model of Internet governance.

A. *The International Covenant on Civil and Political Rights*

In 1948, the UN Commission on Human Rights drafted The Universal Declaration of Human Rights ("UDHR").[25] The UDHR set out thirty articles articulating human rights principles and established the framework for subsequent human rights treatises, such as the ICCPR.[26] After nearly two decades of drafting, the ICCPR went into

24. *See infra* Part III (arguing that an Article 19 analysis should be supplemented by a similar process-based metric).

25. *See History of the Document*, THE UNIVERSAL DECLARATION OF HUM. RTS., http://www.un.org/en/documents/udhr/history.shtml (last visited Dec. 30, 2014) (providing the history of the UDHR) [hereinafter The International Declaration of Human Rights]; SCOTT CARLSON & GREGORY GISVOLD, PRACTICAL GUIDE TO THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS 1-2 (2003) (providing the background of the UDHR).

26. *See* Carlson, *supra* note 25, at 1-2 (providing overview of the ICCPR and UDHR); *see also* THE UNIVERSAL DECLARATION OF HUM. RTS., *supra* note 25.

effect in 1976.[27] The ICCPR requires the signatory State parties to uphold the civil and political rights of individuals, including freedom of religion, speech, assembly, and electoral rights.[28] Currently there are over 160 State Parties, including the United States and the United Kingdom.[29] While China is a signatory of the ICCPR, it has not ratified the treaty.[30]

The ICCPR contains two Optional Protocols.[31] The Optional Protocols are additional sets of rules and procedures to the ICCPR that require separate ratification by a State Party in order to be in effect.[32] In 1976, the First Optional Protocol to the ICCPR provided an avenue for individuals who claim to have suffered a violation of an ICCPR provision to submit complaints to the HRC, granted that the complainant exhausted available domestic remedies.[33] As of April 2014, only 115 parties to the Covenant had adopted the First Optional Protocol.[34]

The Human Rights Committee ("HRC") is the UN-designated body responsible for writing reports about a State's compliance with

---

27. *See* Carlson, *supra* note 25, at 2 (discussing the history of the ICCPR); *The Foundation of International Human Rights Law*, UNITED NATIONS, http://www.un.org/en/documents/udhr/hr_law.shtml (last visited Dec. 31, 2014) (providing the history of ICCPR).

28. *See* ICCPR, *supra* note 5.

29. *See International Covenant on Civil and Political Rights*, UNITED NATIONS TREATY COLLECTION, https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en (last updated Jan. 4, 2014) (noting that there are 168 parties to the ICCPR) [hereinafter *ICCPR Parties*].

30. *See ICCPR Parties*, *supra* note 29 (showing that China has not ratified the treaty); China, CENTER FOR CIVIL AND POLITICAL RIGHTS, http://www.ccprcentre.org/country/china/ (last visited Dec. 30, 2014) (noting that China is not a Party to the ICCPR).

31. There are two Optional Protocols to the ICCPR. The First Optional Protocol is relevant to this Note, and the Second Optional Protocol involves the abolition of the death penalty. *See* Carlson, *supra* note 26, at 2 (providing an overview of the two optional protocols to the ICCPR); *Human Rights Explained: Fact Sheet 5: The International Bill of Rights*, AUSTRALIAN HUM. RTS. COMMISSION (2009), https://www.humanrights.gov.au/human-rights-explained-fact-sheet-5the-international-bill-rights (discussing the Optional Protocols) [hereinafter *ICCPR Fact Sheet 5*].

32. *See* Carlson, *supra* note 25, at 2 (discussing the Optional Protocols); *ICCPR Fact Sheet 5*, *supra* note 31 (explaining how the optional protocols supplement the ICCPR with additional obligations to adopting State Parties).

33. *See* International Covenant on Civil and Political Rights, *opened for signature* Dec. 16, 1966, *available at* http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPCCPR1.aspx [hereinafter First Optional Protocol] (establishing the individual communication procedure).

34. The United Kingdom, People's Republic of China, and the United States have not adopted the First Optional Protocol. *See Optional Protocol to the International Covenant on Civil and Political Rights*, UNITED NATIONS TREATY COLLECTIONS , https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-5&chapter=4&lang=en (last updated Jan. 4, 2014) (listing only 115 parties to the first optional protocol).

the ICCPR.[35] The HRC is not a UN organization per se, but rather an independent expert committee comprised of delegates from State Parties.[36] Utilizing three procedural mechanisms—namely state reporting, individual complaints, and inter-state complaints, the HRC is responsible for examining a member State's compliance with the ICCPR obligations.[37]

As part of the State reporting mechanism, State Parties must submit initial and subsequent periodic reports to inform the HRC about measures undertaken to implement and comply with the ICCPR.[38] The HRC examines these State reports during regularly scheduled sessions and then issues a Concluding Observation, which includes positive observations and concerns regarding State Parties' compliance with the ICCPR.[39] The HRC also encourages compliance with the Covenant by examining specific complaints under the First Optional Protocol.[40] If a violation is found, the HRC may suggest an appropriate remedy.[41] Similar to Concluding Observations, decisions issued by the HRC serve as specific, authoritative interpretations of the ICCPR.[42] It is important to note that the HRC is neither a court

35. *See* Carlson, *supra* note 25, at 2-4 (explaining the role and duties of the HRC); *Monitoring Civil and Political Rights*, UN HUM. RTS. http://www.ohchr.org/EN/HRBodies/CCPR/Pages/CCPRIntro.aspx (last visited Dec. 30, 2014) (describing the role of the Human Rights Committee).

36. Although they share similar names and terminology, the HRC is not the same as the Committee on Human Rights, nor is it part of the Office of the High Commission for Human Rights. *See* Carlson, *supra* note 25, at 2-4.

37. ICCPR, *supra* note 5; *see* Carlson, *supra* note 26, at 2-13 (explaining each procedural mechanism).

38. ICCPR, *supra* note 5.

39. *See* Carlson, supra note 26 at 8-9 (discussing Concluding Observations); *UN Human Rights Committee Issues Concluding Observations on State Reports on Chad, Kyrgyzstan, Latvia, Nepal, Sierra Leone, and the United States*, INT'L JUST. RESOURCE CENTER (Apr. 3, 2014), http://www.ijrcenter.org/2014/04/03/un-human-rights-committee-issues-concluding-observations-on-state-reports-of-chad-kyrgyzstan-latvia-nepal-sierra-leone-and-the-united-states-of-america/ (summarizing the Concluding Observations from the 110th HRC session).

40. *See* First Optional Protocol*, supra* note 33; Carlson, *supra* note 25, at 9-12 (providing an overview of the First Optional Protocol).

41. *See* First Optional Protocol, *supra* note 33 (establishing the framework for State Party member's remedial statements to the HRC).

42. *See* Carlson, *supra* note 25, at 11 (stating that similar to the Concluding Observations on state reports, HRC decisions offer specific, authoritative interpretation of the ICCPR); *Human Rights Treaty Bodies – Individual Communications*, UN HUM. RTS., http://www.ohchr.org/EN/HRBodies/TBPetitions/Pages/IndividualCommunications.aspx (last visited Dec. 30, 2014) [hereinafter *Individual Communications*] ("The Committees' decisions represent an authoritative interpretation of the treaty concerned.").

nor does it possess the executive capacity to enforce the ICCPR.[43] Rather, decisions are used to apply international pressure to a State Party not in compliance.[44]

1. The Expansion of the ICCPR to the Internet

Article 19 of the ICCPR secures the right to expression and opinion free from external repression.[45] It states:

> 1. Everyone shall have the right to hold opinions without interference.
>
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
>
> 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (*ordre public*), or of public health or morals.[46]

Until recently, international human rights law concerning the Internet was sparse.[47] For instance, there is no mention of the Internet, even in passing, in the HRC 2009–2010 report.[48] Article 19 of the

---

43. *See* Carlson, *supra* note 25, at 11 (noting that the Committee is not a court, but it does have interpretative authority grounded in a legally binding treaty obligation); *Civil and Political Rights: The Human Rights Committee Fact Sheet No. 15* (Rev. 1), http://www.ohchr.org/Documents/Publications/FactSheet15rev.1en.pdf (last visited Dec. 30, 2014), [hereinafter *HRC Fact Sheet 15*] (describing that if the HRC finds a violation in a case, the State party is requested to remedy that violation pursuant to the obligation in Article 2, Paragraph 3 of the ICCPR).

44. *See* Carlson, *supra* note 25, at 11 (discussing the effects of HRC decisions); *Individual Communications*, *supra* note 42 (discussing the follow-up procedures after a violation has been found).

45. *See* ICCPR, *supra* note 5, art. 19.

46. *Id*.

47. Molly Land, *Toward an International Law of the Internet*, 54 HARV. INT'L L.J. 393, 396 (2013) (explaining how recent human rights reports have neglected to address the Internet). *See generally* Rep. of the Human Rights Comm., Vol. 1, 97th-99th Sess., Oct. 12-Oct. 30, 2009, Mar. 8-Mar. 26, 2010, July 12-July 30, 2010, U.N. Doc. A/65/40; GAOR, 65th Sess., Supp. No. 40, (2010) [hereinafter HRC 2009-2010 Report] (failing to address any issues regarding the Internet).

48. *See* HRC 2009-2010 Report, *supra* note 47; Land, *supra* note 47, at 397 (discussing the absence of issues relating to the Internet in the 2009-2010 Human Rights Report).

ICCPR provides no explicit protection for Internet access, a concept that did not exist during the drafting process.[49] Nonetheless, scholars argue that the ICCPR explicitly protects expression in the "media," and that the drafters intended to include later-developed technologies, such as the Internet, under Article 19.[50] Scholars have looked to recent HRC reports and publications that recognize the importance of the Internet with respect to the right to freedom of expression.[51] For instance, in his May 2011 report, the Special Rapporteur for Freedom of Expression, Frank La Rue, observed that Article 19 of the UDHR, the precursor to the ICCPR, was drafted with the foresight to include and accommodate future technological developments.[52] Special Rapporteur Frank La Rue wrote that, in light of the importance of the Internet to human rights, "facilitating access to the Internet for all individuals, with as little restrictions to online content as possible,

49. *See* ICCPR, *supra* note 5, art. 19. The Internet was in its infancy in the late 1960s, and it was used primarily for military purposes. Commercial use of the Internet was not widespread until the late 1980s. *See generally Brief History of the Internet*, INTERNET SOCIETY, http://www.Internetsociety.org/Internet/what-Internet/history-Internet/brief-history-Internet (last visited Dec. 30, 2014) (providing the history of Internet development).

50. *See* Human Rights Comm., Gen. Comment No. 34, Art. 19: Freedoms of Opinion and Expression, 102nd Sess., July 11-July 29, 2011, U.N. Doc. CCPR/C/GC/34 (Sep. 12, 2011) (establishing that Article 19(2) protects all means of expression, including web-based modes of expression) [hereinafter UN General Comment 34]; Land, *supra* note 47, at 394 (arguing that although Article 19 does not guarantee a right to the Internet, it explicitly protects the media of expression and information)..

51. *See* Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc. A/66/290 (Aug. 10, 2011) (by Frank La Rue) (declaring that access to the Internet is essential to enjoy the rights enumerated in the ICCPR) [hereinafter August 2011 La Rue Report]; Land, *supra* note 47, at 398-402 (noting the recent scholarly attention regarding the Internet and human rights); .

52. Special Rapporteur on The Promotion and Protection of the Right to Freedom of Opinion and Expression, *Rep. on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, 7, U.N. Doc. A/HRC/17/27, (May 16, 2011) [hereinafter May 2011 La Rue Report] (explaining that as a result of the UDHR drafters' foresight, "the framework of international human rights law remains relevant today and equally applicable to new communication technologies such as the Internet"); *cf.* Land, *supra* note 47, at 402 (utilizing a textual approach, Professor Land interprets the term "media" to include both the form and the channel of expression). A Special Rapporteur is an expert appointed by the HRC to examine and report on a country's situation on a specific area of human rights. Special Rapporteur La Rue was the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression from August 2008 to July 2014. *See Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UNITED NATIONS HUMAN RIGHTS, http://www.ohchr.org/EN/ISSUES/FREEDOMOPINION/Pages/OpinionIndex.aspx (last visited Dec. 30, 2014) (describing the role of the Special Rapporteur).

should be a priority for all states."[53] In addition, his reports condemned certain practices that "cut off access to the Internet entirely" as "disproportionate," thus violating Article 19 of the ICCPR.[54]

Scholars argue that although a "freedom to connect" is not specifically articulated in Article 19(2), the freedom is supported by Article 19's explicit protection of the rights to seek, receive, and impart information.[55] The text of Article 19(2) suggests that every type of expression communicable is protected, subject to the limitations in Paragraph 3 permitting censorship of speech where necessary.[56]

Article 19(3) establishes that limitations on the rights enumerated in Article 19 shall only be provided by law and must be necessary for the respect of the rights or reputations of others, the protection of national security, public order, public health, or morals.[57] Interpreting this provision, Special Rapporteur Frank La Rue articulated the following test:

> Any restriction on expression must be provided by law, which must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and must be made accessible to the public (principles of predictability and transparency);

---

53. *See* May 2011 La Rue Report, *supra* note 52, at 4 (recognizing the importance of the Internet in building democratic societies).

54. Special Rapporteur La Rue was referring to several incidents, including Egypt's 2011 Internet blackout, the "three strikes-law" in France, and the 2010 Digital Economy Act. *See* May 2011 La Rue Report, *supra* note 53, at 10-14.

55. *See* Land, *supra* note 48, at 410. Professor Land also noted that an international "freedom to connect" is also supported by Former Secretary of State of the United States Hillary Clinton's January 2010 Speech. Secretary Clinton articulated that there were additional freedoms that were inherent in the freedoms identified by former United States President Franklin Roosevelt in his 1941 Four Freedoms speech. This "freedom to connect," is predicated on the idea that governments should not limit people from connecting to the Internet or to each other. Hillary Rodham Clinton, Sec'y of State, Remarks on Internet Freedom, (Jan. 21, 2010), (transcript available at http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm) (noting that the freedom to connect is analogous to a freedom of assembly in cyber space).

56. *See* Human Rights Comm., Views on Commc'ns Nos. 359/1989 and 385/1989, U.N. Doc. CCPR/C/47359/1989 and 385/1989/Rev.1 (1993) (May 5, 1993) (finding that Article 19 protects any form of subjective idea or opinion capable of transmission); Carlson, *supra* note 25, at 121 (describing that while Article 19(2) mentions several types of media, it protects expression in any other media).

57. *See* ICCPR, *supra* note 7, art. 19(3).

> The restriction must pursue one of the purposes set out in Article 19(3) of the ICCPR, namely (1) to protect the rights and reputations of others, or (2) to protect national security or of public order, or of public health or morals (principle of legitimacy); and
>
> The restriction must be proven necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality).[58]

International courts have used variations of the three-part test to examine limitations on freedom of expression.[59]

2. Internet Censorship

Internet censorship schemes are commonly divided into two groups: hard censorship and soft censorship.[60] Hard censorship involves a government exercising control over Internet infrastructure or compelling intermediaries to do so through the force of law.[61] Soft censorship, on the other hand, involves employing laws as a pretext to block material, paying for filtered access, or persuading intermediaries to restrict content.[62] Acts of soft censorship, such as withholding state assistance, may be less legitimate because they are not as visible as attempts at hard censorship, such as firewalls and

---

58. May 2010 La Rue Report, *supra* note 52, at 6-7 (explaining the three-part cumulative test*); see* August 2011 La Rue Report, *supra* note 51, at 8 (requiring limitations on freedom of expression to meet the three-part test).

59. *See, e.g.*, Lingens v. Austria, App. No. 9815/82, 8 Eur. H.R. Rep. 407, ¶¶ 39-40 (1986) (Eur. Ct. H.R.) (espousing a standard similar to the three-part test); *see also* Agnes Callamard, *Expert Meeting on the Links Between Article 19 and 20 of the ICCPR: Freedom of Expression and Advocacy of Religious Hatred that Constitutes Incitement to Discrimination, Hostility or Violence*, ARTICLE 19 (Oct. 2-3, 2008), http://www.article19.org/data/files/pdfs/conferences/iccpr-links-between-articles-19-and-20.pdf (discussing the use of the three-part test in international courts).

60. *See* Bambauer, *Orwell's Armchair*, *supra* note 10, at 867 (describing the types of censorship); *Soft Censorship, Hard Impact: A Global Review*, WORLD ASS'N OF NEWSPAPERS AND NEWS PUBLISHERS, at 4-5 (providing an overview of soft censorship).

61. Hard censorship schemes are often blocked by architectural or constitutional constraints. *See* Bambauer, *Orwell's Armchair*, *supra* note 10, at 867.

62. In *Orwell's Armchair*, Professor Bambauer argues that soft censorship is less legitimate than hard censorship because soft censorship models are not transparent, open, or narrowly applied as hard censorship models. *See* Bambauer, *Orwell's Armchair*, *supra* note 10, at 867. S*ee also* Don Podesta, Op-Ed., *The Rise of Soft Censorship*, WASH. POST (Feb. 2, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/02/01/AR2009020101671.html (discussing an Illinois politician's threat of withholding state assistance from a newspaper's parent company if the company did not fire specific members of the editorial board who were critical of him).

explicit censorship laws.[63] For instance, after Hong Kong newspaper publisher Next Media printed several articles opposing a proposed security law in China, the company lost considerable advertising revenue when the People's Republic of China ("PRC") pressured companies not to do business with the company.[64]

Filtering utilizes technological systems to prevent end-users from receiving specific content.[65] While the act of filtering is a form of hard censorship, it can also be the result of attempts at soft censorship.[66] Internet filters have been implemented at various levels, from the physical network infrastructure, forming the backbone of the Internet-to-Internet service providers ("ISPs"), private networks, and individual computers.[67] During the early 1990s, there were commonly two types of Internet filters: the inclusion filter and the exclusion filter.[68] Inclusion filters typically use "white lists" to include websites that are permitted for browsing, whereas an exclusion filter employs a

63. *See* Bambauer, *Orwell's Armchair*, *supra* note 10, at 868 (discussing why soft censorship is often less legitimate than hard censorship); Podesta Op-Ed, *supra* note 62 (discussing various forms of indirect censorship).

64. Don Podesta, *Soft Censorship: How the Government Around the Globe Use Money to Manipulate the Media*, CENTER FOR INT'L MEDIA ASSISTANCE (Jan. 9, 2009), http://www.academia.edu/3651678/Soft_Censorship_How_Governments_Around_the_Globe_Use_Money_to_Manipulate_the_Media (reporting the PRC's use of indirect economic pressures to chill speech); Podesta Op-Ed, *supra* note 62 (reporting on the PRC's indirect censorship).

65. An end-user is the person that uses the finished product, and is differentiated from other types of users, such as developers, installers, and servicers. *See Definition: End User*, WHATIS, (Apr. 2005), http://whatis.techtarget.com/definition/end-user; *What are Internet Filters?*, MICROSOFT, http://www.microsoft.com/en-GB/security/resources/internetfilters-whatis.aspx (last visited Dec. 30, 2014) (explaining the role and properties of Internet filters).

66. *See* Bambauer, *Orwell's Armchair*, *supra* note 10, at 889-91 (discussing United States Congress' use of subsidies to implement filters in US public schools and libraries); *also Internet Filtering as a Form of Soft Censorship*, COMPUTERWORLD (Mar. 19, 2010), http://www.computerworld.com/article/2468012/endpoint-security/internet-filtering-as-a-form-of-soft-censorship.html (discussing the effects of the Children's Internet Protection Act).

67. *See* Marc D. Nawyn, *Code Red: Responding to the Moral Hazards Facing U.S. Information Technology Companies in China*, 2007 COLUM. BUS. L. REV. 505, 511 (describing the implementation of Internet filtering in a variety of access points); *About Filtering*, OPENNET INITIATIVE, https://opennet.net/about-filtering (last visited Apr. 5, 2015) (overview of Internet filtering).

68. *See* Nawyn, *supra* note 67, at 510 (describing inclusion and exclusion filters); *see also* Marjorie Heins & Christina Cho, *Internet Filters: A Public Policy Report, Free Expression Policy Project,* NAT'L COALITION AGAINST CENSORSHIP (2001), *available at* http://ncac.org/wp-content/uploads/import/Internet%20Filter.pdf (describing early Internet Filters).

"blacklist" which specifies websites that users are prohibited from visiting.[69]

Currently, Internet filtering technology has progressed towards using "content analysis" in place of whitelists and blacklists.[70] Filters utilizing content analysis prevents users from accessing any site containing specified keywords, phrases, or even images.[71] This provides two key advantages to censors over the traditional exclusion and inclusion filters.[72] First, unlike traditional filters, content analysis filters do not need to be regularly updated with URL lists.[73] Secondly, content analysis filters maintain greater accuracy than filters that block sites at the IP address level.[74] As a result of its targeted blocking, content analysis filters allow users to receive data from sites that would otherwise be blocked altogether by traditional filters.[75] Content analysis filters have been compared to "censoring out individual sentences within books, as opposed to censoring entire books themselves."[76]

B. *Internet Censorship: The United States*

1. The Onset of Internet Censorship in the United States

Over the course of US history, the First Amendment of the US Constitution has developed into a bulwark against government

---

69. *See* Ronald J. Deibert & Nart Villeneuve, *Firewalls and Power: An Overview of Global State Censorship of the Internet*, *in* HUMAN RIGHTS IN THE DIGITAL AGE 112, 112 (Andrew Murray & Mathias Klang eds., 2004) (describing exclusion and inclusion filters); Nawyn, *supra* note 67, at 511-12 (explaining the difference between white and black lists).

70. *See* Nawyn, *supra* note 67, at 511 (discussing the trend towards content analysis filters); *see also* Jyh-An Lee & Ching-Yi Liu, *Forbidden City Enclosed by the Great Firewall: The Law and Power of the Internet Filtering in China*, 13 MINN. J.L. SCI & TECH. 125, 131 (2012) (describing China's adoption of content-analysis filters).

71. *See* Nawyn, *supra* note 67, at 511 (explaining how content analysis filters operate); Deibert, *supra* note 70, at 112 (describing the capabilities of content analysis filters).

72. *See, e.g.*, Nawyn, *supra* note 67, at 511 (explaining the advantages of content analysis filters over exclusion and inclusion filters); *Real-time Content Analysis*, BLOXX, http://www.bloxx.com/product-technical-info/1/real_time-content-analysis (last visited Apr. 5, 2015) (comparing the key differences of their content analysis filters and traditional exclusion filters).

73. *See supra* notes 68-72 and accompanying text (comparing the differences between content analysis filters and traditional filters).

74. *See, e.g.*, Deibert, *supra* note 69, at 113 (discussing the advantages of content analysis filters); Nawyn, *supra* note 68, at 511-13 (describing the benefits of content analysis filtering).

75. *See* Deibert, *supra* note 70 at 113; Nawyn, *supra* note 67, at 511-13.

76. *See* Deibert, *supra* note 70 at 113; Nawyn, *supra* note 67, at 511-13.

attempts at censorship.[77] Despite the First Amendment and the decentralized nature of the Internet, in 1996, the US Congress made its first attempt to regulate Internet content with the Communications Decency Act ("CDA").[78] Section 223(d) (1) criminalized the use interactive computer services to knowingly transmit "patently offensive" communications to children under the age of eighteen.[79] In *American Civil Liberties Union v. Reno*, the American Civil Liberties Union ("ACLU") sought a preliminary injunction against the enforcement of the CDA in the District Court for the Eastern District of Pennsylvania, arguing, inter alia, that the CDA was unconstitutionally vague and failed to define "indecent" and "patently offensive."[80] The District Court ultimately found that the CDA's effect on the protected speech of adults was "too intrusive to be outweighed by the government's asserted interest . . . in protecting minors from access to indecent material."[81] Consequently, the District Court held that the CDA was facially unconstitutional.[82]

Agreeing with the District Court's findings, the Supreme Court struck down § 223 of the CDA.[83] Justice Stevens, writing for the majority, explained that the Act was unconstitutionally vague, and that the ambiguous language rendered the CDA inconsistent with the purposes of the First Amendment.[84] Justice Stevens further noted that the lack of definitions for both "patently offensive" and "indecent" creates ambiguity about the relationship between the two standards.[85]

In response to the Supreme Court's decision in *Reno*, Congress passed the Child Online Protection Act ("COPA") in 1998.[86] COPA

---

77. Modern First Amendment jurisprudence has greatly expanded what was traditionally regarded as "speech." *See Ashcroft v. Free Speech Coal.*, 535 U.S. 234, 244 (2002). Justice Kennedy, writing for the majority, regarded the First Amendment as a "vast and privileged sphere." *Id.*; *see also* Blake Covington Norvell, *The Modern First Amendment and Copyright Law*, 18 S. CAL. INTERDISC. L.J. 547, 549-52 (2009) (arguing that the modern First Amendment doctrine is more than a doctrine against prior restraints)

78. Communication Decency Act of 1996, 47 U.S.C. § 223 (1996), *invalidated by* Reno v. Am. Civil Liberties Union, 521 U.S. 844 (1997) [hereinafter CDA].

79. CDA § 223(d)(1)(A). *See* ACLU v. Reno, 929 F. Supp. 824, 829 (E.D. Pa. 1996) (providing an overview of the statutory provisions at issue) *aff'd,* 521 U.S. 844 (1997).

80. *Reno*, 929 F. Supp. at 826-28.

81. *Id.* at 855.

82. *Id*. at 883.

83. *Reno*, 521 U.S. at 875.

84. *Id.* at 870.

85. *Id.* at 871.

86. Child Online Protection Act, 47 U.S.C.A. § 231 (1998), *invalidated by* Am. Civil Liberties Union v. Mukasey*,* 534 F.3d 181 (3d Cir. 2008) [hereinafter COPA].

revised the CDA's prior proscription of transmitting indecent communciations to individuals under the age of eighteen to prohibiting such communications toindividuals under the age of seventeen.[87] The scope of COPA was narrowed in its application to the "World Wide Web" and commercial sites.[88] Furthermore, the revised statute prohibits material that is "harmful to minors" rather than "indecent material."[89] Both the CDA and COPA provided an affirmative defense to Internet publishers that implemented access restrictions through age verification and credit card requirements.[90]

Presently, COPA has been effectively disabled after a rally of legal battles.[91] In 1998, similar to the CDA, the ACLU challenged COPA the day President Clinton signed it into law.[92] The Eastern District of Pennsylvania subsequently granted an initial preliminary

87. *Compare* COPA § 231(e)(7) (defining "minor" as any person under 17 years of age), *with* CDA § 223 (prohibiting transmissions of indcent communcaitions to individuals under 18 years of age).

88. *Compare* COPA § 231 (a)(1) ("[B]y means of the World Wide Web"), *with* CDA § 223(h)(1)(C) ("[T]ransmitted, in whole or in part, by the Internet"). The World Wide Web should not be conflated with the Internet. The World Wide Web is a separate platform that utilizes the Internet to transmit data. *See* Keith Wagstaff, *The Internet and the World Wide Web Are Not the Same Thing*, NBC NEWS (Mar. 12, 2014), http://www.nbcnews.com/tech/Internet/Internet-world-wide-web-are-not-same-thing-n51011 (describing the difference between the World Wide Web and the Internet).

Compare COPA § 231(e)(2)(A)-(B) (limiting the scope to commercial websites), *with* CDA § 223 (prohibiting all transfer of the obscene and offensive content to minors).

89. CDA § 223 encountered fatal scrutiny in *Reno* because, among other things, "indecent" was not defined. *Reno*, 521 U.S. at 871. COPA, on the other hand, utilizes the *Miller* test to determine whether the content is obscene. Ashcroft v. ACLU, 535 U.S. 564, 570 (2002). The expression is obscene if:

> (1) . . . the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, that the material is designed to appeal to the prurient interests; (2) it depicts, describes or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breasts; and (3) taken as a whole lacks serious literary, artistic, political or scientific value for minors.

Miller v. California, 413 U.S. 15 (1973) (establishing the *Miller* or "Three-Prong Obscenity" Test).

90. CDA. § 223(e); COPA U.S.C. § 231(c)-(d).

91. *See infra* notes 92-94 and accompanying text (discussing the procedural history of the "COPA cases").

92. *See* ACLU v. Reno, 31 F. Supp. 2d 473 (E.D. Pa. 1999) *aff'd*, 217 F.3d 162 (3d Cir. 2000), *vacated sub nom.*, Ashcroft v. ACLU, 535 U.S. 564 (2002) (enjoining the enforcement of COPA after President Clinton signed it into law on Oct. 21, 1998); *The Legal Challenge to the Child Online Protection Act*, ELECTRONIC PRIVACY INFO. CENTER, http://epic.org/free_speech/copa/ (last visited Dec. 30, 2014) (describing the procedural history of *ACLU v. Reno*).

injunction against government enforcement of COPA.[93] After several appeals and a remand, in 2009 the Supreme Court of the United States finally refused to grant the government's petition for writ of certiorari, which conclusively disabled COPA.[94]

In another attempt to protect children from inappropriate content on the Internet, the US Congress passed the Children's Internet Protection Act ("CIPA") in 2000.[95] Departing from CDA and COPA's punitive approach, CIPA conditioned a school or library's receipt of certain federal funding on the implementation of protective measures, namely Internet filters.[96] The protective measures were required to restrict access to material containing visual depictions of child pornography or material that is obscene or harmful to minors.[97] CIPA also allows authorized library personnel to disable the filtering software for "bona fide research or other lawful purposes."[98] In 2003, the Supreme Court held that CIPA, at least facially, did not violate the First Amendment.[99] Justice Kennedy reasoned that the filtering policy did not burden constitutionally protected speech if an adult could simply ask a librarian to disable the filter without delay.[100]

---

93. *Reno,* 31 F. Supp. 2d at 499.

94. *See* Mukasey v. ACLU*,* 129 S. Ct. 1032 (2009) (mem.); Scott Nicholas, *COPA Child-Porn Law Killed*, PCWORLD (Jan. 22, 2009, 8:00 AM) http://www.pcworld.com/article/158131/copa_killed.html (reporting the end of COPA).

95. The CIPA affects two federal grant statutes. Children's Internet Protection Act of 2001, (CIPA) Pub. L. No. 106-554, §§ 1701-1741, 114 Stat. 2763 (2000) (codified at 20 U.S.C.A. § 9134 (2010) and 47 U.S.C.A. § 254(h) (2008)). The Library Services and Technology Act ("LSTA") authorizes grants to state library administrative agencies to, inter alia, assist libraries in accessing information through the Internet and to pay costs for libraries to acquire and share computer systems and telecommunication technology. *See* Omnibus Consolidated Appropriation Act of 1997. Pub. L. No. 104–208 Title II, § 212, 110 Stat. 3009-295 (1996)_(codified at 20 U.S.C.A. § 9121 (2010))

The E-Rate program established by the Telecommunications Act of 1996 provides qualifying libraries a discount to Internet access. *See* Telecommunications Act of 1996. Pub. L. No. 104-104, § 254, 110 Stat. 71 (1996) (codified in 47 U.S.C.A § 254(h)(1)(b) (2008)); Amitai Etzioni, *On Protecting Children from Speech*, 79 CHI.-KENT L. REV. 3, 15 (2004) (providing an overview of CIPA).

96. 20 U.S.C.A § 9134(f)(A) (2010); 47 U.S.C.A § 254(h)(6)(B)(i) (2008). Congress became concerned that federal funds were being used to facilitate access to pornography. *See* S. REP. NO. 106–41, at 2 (1998) ("[Pornography] may be accessed directly and intentionally, or may turn up as the unintended product of a general Internet search.").

97. 20 U.S.C.A. § 9134(f)(1)(A) (2010); 47 U.S.C.A § 254(h)(6)(B)(i) (2008)

98. 20 U.S.C.A § 9134(f)(3) (2010); 47 U.S.C.A § 254(h)(6)(D) (2008)

99. *See* United States v. Am. Library Ass'n, Inc., 539 U.S. 194 (2003).

100. *See id.* at 214.

In the United States, telecommunication companies own and operate a significant majority of the Internet's infrastructure.[101] Nonetheless, various US agencies regulate the Internet in some capacity. For instance, the Department of Homeland Security protects the integrity of the infrastructure from natural disasters and cyber-attacks.[102] The Federal Trade Commission ("FTC") monitors online advertising and tracking.[103] In 2010, the Federal Communication Commission ("FCC") released an "Open Internet" Order mandating that ISPs not block lawful content and services, subject to reasonable network management, and requiring ISPs to not unreasonably discriminate against transmission of lawful traffic.[104] However, on January 14, 2014, the US Court of Appeals for the District of Columbia struck down the core non-discriminatory provision of the 2010 Order.[105]

2. US Copyright Laws and Their Chilling Effects

Scholars have argued that copyright laws inherently affect freedom of speech.[106] However, copyright laws are permitted even in

---

101. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, INTERNET INFRASTRUCTURE: CHALLENGES IN DEVELOPING A PUBLIC/PRIVATE RECOVERY (October 23, 2007), *available at* http://www.gao.gov/assets/120/118189.pdf (discussing that vast majority of its infrastructure is currently owned and operated by the private sector).

102. *See id*. (reporting DHS' plans in coordinating with private industry infrastructure stakeholders to produce various Internet recovery-related plans). *See generally Court Rules Dept. of Homeland Security Must Reveal 'Internet Kill Switch' Protocol*, RT, (Nov. 17, 2013, 2:19 AM) http://rt.com/usa/homeland-security-Internet-kill-switch-742/ (reporting the District Court's decision to require DHS to reveal its rumored capabilities to shut down the Internet during national crises).

103. *See* Press Release, FTC, FTC Staff Revises Online Behavioral Advertising Principles, (Feb. 12, 2009), *available at* http://www.ftc.gov/news-events/press-releases/2009/02/ftc-staff-revises-online-behavioral-advertising-principles (reporting the FTC's recent revision to balance the potential benefits of behavioral advertising against the privacy concerns).

104. Many dubbed the FCC Order as the net-neutrality order because it prevented discrimination based on content. *See Open Internet*, FCC, http://www.fcc.gov/openInternet (last visited Dec. 30, 2014) (discussing the principle of net-neutrality).

105. While the Court of Appeals upheld the transparency requirement of the FCC order, the court struck down the anti-blocking and nondiscrimination provisions to broadband providers. Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014).

106. *See* Erwin Chemerinsky, *Balancing Copyright Protections and Freedom of Speech: Why the Copyright Extension Act Is Unconstitutional*, 36 LOY. L.A.L. REV. 83 (2002) (providing a general overview of the copyright law vis-à-vis the First Amendment); David S. Olson, *First Amendment Interests and Copyright Accommodations*, 50 B.C. L. REV. 1393, 1395 (2009) (discussing the inherent tension between the First Amendment's community right to hear and copyright law).

societies that value the free exchange of expression because copyright laws are seen overall as enhancing expression by incentivizing new creations and publications.[107] On March 1, 1989, the United States became a party to the Berne Convention for the Protection of Literary and Artistic Works (the "Berne Convention"), an international agreement governing copyrights.[108] In efforts to expand the scope of the Berne Convention, a 100-year-old copyright agreement, to the digital era, members of the World Intellectual Property Organization ("WIPO") adopted the World Intellectual Property Organization Copyright Treaty ("WIPO Treaty") in 1996.[109] The WIPO Treaty requires members to, among other things, establish adequate legal protection against the circumvention of technological protections used by authors in protecting their works.[110] However, US implementation of the WIPO Treaty resulted in unforeseen chilling effects on Internet speech.[111]

In 1998, the US Congress enacted the Digital Millennium Copyright Act ("DMCA") in accordance with the WIPO treaty.[112] Specifically, the Online Copyright Infringement Liability Limitation

---

107. *See* Eldred v. Ashcroft, 537 U.S. 186, 219 (2003) (recognizing that copyright laws spur the creation and publication of new expressions); Chemerinsky, *supra* note 108, at 83 (discussing how copyright law may be consistent with the First Amendment when it exists to encourage the creation and distribution of more speech).

108. The United States became a party to the Berne Convention through the adoption of The Berne Convention Implementation Act of 1988. 17 U.S.C. § 101 (1988). The Berne Convention was first accepted in Berne, Switzerland, in 1886. *See* Binyomin Kaplan, *Determining Ownership of Foreign Copyright: A Three-Tier Proposal*, 21 CARDOZO L. REV. 2045, 2050 n.20 (2000) (noting that Berne Convention was originally signed by ten nations in 1886).

109. World Intellectual Property Organization Copyright Treaty art. 11, Dec. 20, 1996, S. Treaty Doc. No. 105-17 (1997), 36 I.L.M. 65 (1997) [hereinafter WIPO Treaty]; *see WIPO Treaties - General Information*, WORLD INTELL. PROPERTY ORG., http://www.wipo.int/treaties/en/general/ (last visited Dec. 30, 2014) (providing the history of the WIPO).

110. *See* WIPO Treaty, *supra* note 109, at art. 11 (requiring members to provide legal protections and remedies against the circumvention of technological measures); *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 440 (2d Cir. 2001) (discussing that the DMCA was enacted in compliance with the WIPO treaty).

111. *See Unintended Consequences: Fifteen Years under the DMCA*, ELECTRONIC FRONTIER FOUND. (March 2013), https://www.eff.org/pages/unintended-consequences-fifteen-years-under-dmca (discussing the DMCA's effect on Internet speech); *infra* notes 275-92 (describing the DMCA's chilling effect).

112. *See* H.R. REP. No. 105-551, at 1 (1998) (discussing the implementation of the WIPO treaty and Performances and Phonograms Treaty); David L. Hitchcock & Kathy E. Needleman, *Current Status of Copyright Protection in the Digital Age and Related Topics*, 8 TEX. WESLEYAN L. REV. 539, 550-54 (2002) (providing a brief overview of the DMCA).

Act ("OCILLA") codified Title II of the DMCA.[113] Title II, commonly referred to as "§ 512," protects service providers by establishing a "safe harbor," which limits the service's intermediary liability for the copyright infringement of its users provided that the service provider implements copyright policies and a notice-and-takedown system.[114] Upon receiving notice, a service provider must promptly remove or block access to the material in order to qualify for the § 512 safe harbor.[115]

Generally, the DMCA's system of counter-notification forces the online poster to reassert the lawfulness of his speech.[116] For example, if a subscriber provides a proper "counter-notice" claiming that the material does not infringe a copyright, the service provider must then promptly notify the claiming party of the individual's objection.[117] By providing a "counter-notice," however, the counter-notifier must submit, among other things, her name and address to the service provider.[118] This presents a problem for Internet users who want to remain anonymous. For instance, suspected terrorist organizations have used DMCA takedowns of YouTube videos critical of Islam in efforts to obtain the uploader's address and name.[119]

---

113. *See* 17 U.S.C.A, § 512 (2010); Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 26-28 (2012) (providing factual background of the DMCA Safe Harbor); *see also* S. Rep. No. 105-190, at 2 (1998) (addressing the need of a safe harbor provision).

114. *See* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 231 (Jonathan Zittrain et al. eds., 2008) (discussing the nature of § 512 safe harbor provision). § 512 was intended to balance the need for swift, methodic response to potential infringement with the rights of the content-poster. *See* S. Rep. No. 105-190, at 18 (1998) (discussing concerns regarding the application of § 512).

115. *See* 17 U.S.C.A. § 512(c)(1) (2010); Jennifer M. Urban & Laura Quilter, *Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act,* 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 621, 625-26 (2006) (describing the 512 takedown mechanism).

116. *See* Wendy Seltzer, *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment*, 24 HARV. J.L. & TECH. 171, 177 (2010) (explaining that the added cost operates as censorship). *But see* Bambauer, *Cybersieves*, *supra* note 21, at 401 (recognizing that there is value in the DMCA's citizen-participatory process).

117. 17 U.S.C.A. § 512(g)(2)(B)-(C) (2010); *see Question: What are the Counter-Notice and Put-Back Procedures?*, CHILLING EFFECTS, http://www.chillingeffects.org/question.cgi?QuestionID=132 (last visited Dec. 30, 2014) (describing § 512 counter-notice and put-back procedures).

118. 17 U.S.C.A. § 512(g)(3)(D) (2010).

119. *See* Stephen Doble, *Youtubers Targeted by Terrorists After Copyright Claim*, VIDEOTER (Nov. 6, 2014), http://videoter.com/youtubers-targeted-by-terrorists-after-dmca-claim/ (reporting the suspected use of DMCA takedowns by terrorist organizations); Paul Tamburro, *Terrorists Hunt Down Youtuber Using Information From Fake DMCA Claim*, CRAVEONLINE (Nov. 6, 2014), http://www.craveonline.com/lifestyle/tech-and-gadgets-news/

3. SOPA and PIPA: The Menacing Twins

Recently, Congress encountered the ire of Internet users, tech companies, and scholars with the proposal of the Stop Online Privacy Act ("SOPA") and its Senate counterpart, Protect Internet Property Act ("PIPA").[120] SOPA was directed towards websites that are "dedicated to the theft of US property."[121] Under section 102(a), a foreign website is deemed to be a "foreign infringing site" if:

> (1) the Internet site or portion thereof is a U.S.-directed site and is used by users in the United States;
>
> (2) the owner or operator of such Internet site is committing or facilitating the commission of criminal violations punishable under . . . Title 18, United States Code; and
>
> (3) the Internet site would, by reason of acts described in paragraph (1), be subject to seizure in the United States in an action brought by the Attorney General if such site were a domestic Internet site.[122]

In practice, a foreign website hosting user-generated content may be deemed an "infringing site" under § 102 simply because of the allegedly infringing acts of a single user.[123]

SOPA has the potential to fundamentally change the current DMCA notice-and-takedown regime without providing adequate due process.[124] The language in § 102 and § 103 of the bill grants complainants or the Attorney General the ability to stop online advertisers and credit card processors from doing business with the

---

785199-terrorists-hunt-youtuber-using-information-fake-dmca-claim (reporting that a Youtuber is hiding from suspected terrorists after sharing his information pursuant to the DMCA counter-notification procedures).

120. Stop Online Piracy Act, H.R. Bill 3261, 112th Cong. (2011); Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011, S. Bill 968, 112th Cong. (2011).

121. H.R. 3261 § 103; *see* Jan André BlackBurn-Cabera, *Streaming Movies Online: The E! True Hollywood Story* 5 U. PUERTO RICO BUS. L.J. 59, 86 (2014).

122. H.R. 3261 § 102(a).

123. Note H.R. 3261 § 102(a)'s lack of any intent or knowledge requirement. *See id.* A foreign website can be deemed an infringing site without inducement or knowledge of the criminal infringement by site's operator. *See id; see also* Luke Johnson, *What is SOPA? Anti-Piracy Bill Explained*, THE HUFFINGTON POST (Jan. 19, 2012), http://www.huffingtonpost.com/2012/01/19/what-is-sopa_n_1216725.html#s620431title=Rep_Keith_Ellison (last visited Dec. 30, 2014) (reporting the effects of SOPA).

124. *See infra* notes 125-26 and accompanying text (explaining SOPA's notice procedure).

targeted website, by the mere act of filing a unilateral complaint.[125] For example, if PayPal receives notice from a complainant, PayPal has five days to disable its financial services with the alleged website in order to be protected under the law.[126]

A host of critics have argued that SOPA would negatively impact US cybersecurity and violate the First Amendment.[127] The Electronic Freedom Foundation, an international organization that deals with legal issues in the digital world, argues that SOPA essentially allows the Attorney General to blacklist companies from doing business using the web.[128] Constitutional scholar Laurence H. Tribe argues that the notice-and-termination procedure of § 103(a) is inconsistent with "prior restraint" doctrine.[129] In US First Amendment jurisprudence, prior restraint occurs when restrictions are placed on expression before the expression occurs.[130] Section 103(a) delegates to a private party the power to suppress speech without prior notice and a judicial hearing.[131]

---

125. H.R. Bill 3261 §§ 102(c), 103(b); *see* BlackBurn-Cabera, *supra* note 122, at 86 (explaining that SOPA would have allow the removal of copyright infringing content from websites without providing adequate procedures for websites to defend themselves).

126. *See* H.R. 3261 § 103(b).

127. *See Growing Chorus of Opposition to "Stop Online Piracy Act"*, CENTER FOR DEMOCRACY AND TECH. (Nov. 4, 2011), https://www.cdt.org/report/growing-chorus-opposition-stop-online-piracy-act (listing concerns and complaints of a growing chorus of opposition to SOPA); Tim Hornyak, *Blare Your Dissent with Anti-SOPA Ringtones*, CNET (Jan. 18, 2012), http://www.cnet.com/news/blare-your-dissent-with-anti-sopa-ringtone/ (reporting one way to protest against SOPA and PIPA).

128. Trevor Timm, *The Stop Online Piracy Act: A Blacklist by Any Other Name is Still A Blacklist*, ELECTRONIC FRONTIER FOUND. (Nov. 7, 2012), https://www.eff.org/deeplinks/2011/11/stop-online-piracy-act-blacklist-any-other-name-still-blacklist (discussing how the bill gives the Attorney General the power to essentially blacklist companies from doing business on the Internet); *see* Parker Higgins, *What's On the Blacklist? Three Sites That SOPA Could Put at Risk*, ELECTRONIC FRONTIER FOUND. (Nov. 15, 2012), https://www.eff.org/deeplinks/2011/11/whats-blacklist-three-sites-sopa-could-put-risk (discussing three sites that may be negatively affected by SOPA).

129. Laurence H. Tribe is a Professor of Constitutional Law at Harvard Law School. *See* Lawerence H. Tribe, *The "Stop Online Piracy Act" (SOPA) Violates The First Amendment*, SERENDIPITY (last visited Dec. 30, 2014), http://www.serendipity.li/cda/tribe-legis-memo-on-SOPA-12-6-11-1.pdf (arguing that SOPA violates the First Amendment because the language of the bill is impermissibly vague and amounts to prior restraint).

130. *See, e.g.*, Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 70 (1963) (invalidating a Rhode Island law that created an extrajudicial committee based on the prior restraint doctrine); *see* Robert Plotkin, *Fighting Keywords: Translating the First Amendment to Protect Software Speech*, 2003 U. ILL. J.L. TECH. & POL'Y 329, 389 (Fall 2003) (describing the use of prior restraint doctrine in respect to circumvention software).

131. *See* H.R. 3261 § 102(a); Tribe, *supra* note 129 (arguing that section 102 amounts to a form of extrajudicial prior restraint).

Similar to its twin bill in the US House of Representatives, SOPA, PIPA authorizes a private right of action for copyright holders against alleged infringing websites.[132] However, unlike SOPA, PIPA limits its target to websites with "no significant use other than engaging in, enabling, or facilitating the reproduction, distribution, or public performance of copyrighted works . . . ."[133]

On November 15, 2011, several tech giants placed a full-page advertisement in the New York Times telling members of Congress that they do not support the language of the bills.[134] On January 18, 2012, English Wikipedia, Reddit, Google, and others temporarily shut down or altered their websites in order to protest SOPA and PIPA.[135] Facing large opposition from the Internet and tech community, US House of Representative Lamar Smith stated that "[t]he House Judiciary Committee [would] postpone consideration of the legislation until there is a wider agreement on a solution."[136]

In sum, the US legislation-based model is largely influenced by concerns of protecting property rights and minors from obscenity.[137]

---

132. S. Bill 968, 112th Cong. § 3 (2011).

133. *See* Mike Masnick, *Full Text Of The PROTECT IP Act Released: The Good, The Bad And The Horribly Ugly*, TECHDIRT (May 11, 2011), http://www.techdirt.com/articles/20110511/00115314234/full-text-protect-ipact-released-good-bad-horribly-ugly.shtml (discussing pros and cons of PIPA). *Compare* H.R. 3261 § 102 (broadly defining a foreign infringing websites), *with* S. Bill 968 § 2 (defining "Internet site dedicated to infringing activities" as a website with "no significant use other than engaging in, enabling, or facilitating the reproduction, distribution, or public performance of copyrighted works . . . .").,

134. *See* Andrew Couts, *Internet Titans Fight SOPA With Full-Page NY Times Ad*, DIGITAL TRENDS (Nov. 17, 2011), http://www.digitaltrends.com/web/internet-titans-fight-sopa-with-full-page-ny-times-ad/; Cory Doctorow, *Internet Giants Place Full-Page Anti-SOPA Ad in NYT*, BOINGBOING (Nov. 16, 2011), http://boingboing.net/2011/11/16/Internet-giants-place-full-pag.html.

135. *See* Tom Cheredar, *SOPA Blackouts and Protests Go Live (Gallery of Screenshots)*, VENTUREBEAT (Jan. 17, 2012), http://venturebeat.com/2012/01/17/sopa-protests-go-live (reporting that Google updated its homepage with a large sideways black box over the company's logo); *SOPA Protests Planned by Google, Wikipedia and Others on Jan. 18*, WASH. POST, (Jan. 17, 2012), http://www.washingtonpost.com/business/economy/sopa-protests-planned-by-google-wikipedia-and-others-on-jan-18/2012/01/17/gIQALKBL6P_story.html (reporting the companies' objection to language in the bills that grant the United States Government the right to block entire Web sites with copyright-infringing content).

136. Johnathan Weisman, *After an Online Firestorm, Congress Shelves Antipiracy Bills*, N.Y. TIMES, Jan. 20, 2012, at B6, *available at* http://www.nytimes.com/2012/01/21/technology/senate-postpones-piracy-vote.html?_r=0 (reporting that congressional leaders shelved PIPA and SOPA after facing vehement opposition).

137. *See supra* notes 78-136 and accompanying text (describing the various legislations that regulate Internet content).

In addition, compared to other countries, the US model relies on a system of removal through private action rather than blacklisting or blocking.[138] Despite numerous legislative attempts to regulate speech on the Internet, the United States still maintains one of the world's most robust protections for freedom of speech.[139] The core value of freedom of expression is further evident in community protests against bills such as SOPA and PIPA.[140] Despite the United States' constitutional protections of speech, the chilling effects caused by the country's copyright laws run afoul of the spirit of Article 19.[141]

C. *United Kingdom: Watchdogs and the End of Cyber-Libertarianism*

Compared to the United States, the United Kingdom has a hands-off approach to regulating Internet content.[142] The UK model of Internet governance involves, among other things, citizen-participation and cooperation between private and government agencies.[143]

---

138. *See supra* notes 106-119 and accompanying text (discussing the DMCA's notice-and-takedown procedure); *see also* Zittrain, *supra* note 114, at 226 (describing that US content restriction relies more on the removal of content rather than blocking).

139. *See, e.g.*, Jeremy Maltby, *Juggling Comity and Self-Government: The Enforcement of Foreign Libel Judgments in U.S. Courts*, 94 COLUM. L. REV. 1978, 1979 (1994) (comparing the speech-protective standard employed by the United States to countries such as Britain and Canada, which have libel laws that favor plaintiffs' interest in privacy and reputation at the expense of freedom of the press); Timothy Zick, *Territoriality and the First Amendment: Free Speech at-and Beyond-Our Borders*, 85 NOTRE DAME L. REV. 1543, 1585 (2010) (discussing that plaintiffs have obtained judgments against US authors under foreign libel laws that are less speech protective than US laws).

140. *See supra* notes 134-36 and accompanying text (discussing the community protests against SOPA and PIPA).

141. *See* May 2011 La Rue Report, *supra* note 52, at 11-12 (arguing that the current system of notice-and-takedown systems, such as the DMCA, is subject to abuse by State and private actors); *Internet Intermediaries*, *supra* note 18, at 10 (discussing comments by international bodies on intermediary liability regimes).

142. *See* Open Net Initiative: United Kingdom, OPEN NET INITIATIVE, 357 (Dec. 18 2010), *available at* https://opennet.net/sites/opennet.net/files/ONI_UnitedKingdom_2010.pdf (noting that the UK's "no-table libertarian tradition" is manifested by its solid guarantees of freedom of expression, freedom of information, and protection of privacy) [hereinafter ONI UK Report]. *See generally*, Keen, *supra* note 20, at 368 (discussing that the United Kingdom's 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 want to see).

143. *See* Keen, *supra* note 20, at 368; *infra* notes 150-160 and accompanying text (discussing the UK government's cooperation with the Internet Watch Foundation).

As a member of the European Union, the UK has implemented the bloc's directives into law.[144] For instance, the UK incorporated provisions of the European Convention of Human Rights ("ECHR") into the UK Human Rights Act of 1998.[145] Similar to Article 19 of the ICCPR, Article 10 of the EHCR contains a right to the freedom of expression and allows restrictions that are "in accordance with law" and "necessary in a democratic society."[146]

1. The Internet Watch Foundation

In 1996, the UK Metropolitan Police reported that child pornography was surfacing on newsgroups, a type of forum with discussion of a particular topic.[147] The Department of Trade & Industry, led discussions with Internet Service Provider Association ("ISPA"), Home Office, Metropolitan Police, and Safety-Net Foundation, concerning the proliferation of illegal content on the newsgroups.[148] The result of the discussions was the creation of the R3 Safety Net Agreement, which in turn formed the Internet Watch Foundation ("IWF").[149]

The IWF is an independent non-government organization, which receives support from the UK government.[150] The IWF is tasked with

---

144. *See* ONI UK Report, *supra* note 142, at 357 (noting that EU's law takes precedence over national law); *Q&A: How UK Adopts EU Laws*, BBC (Jul. 21, 2009), http://news.bbc.co.uk/2/hi/europe/8160808.stm (explaining how the United Kingdom adopts EU legislation).

145. Human Rights Act, 1998, c. 42. (U.K.).

146. European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 10, Nov. 4, 1950, 213 U.N.T.S. 221.

147. *See IWF History*, INTERNET WATCH FOUND., https://www.iwf.org.uk/about-iwf/iwf-history (last visited Dec. 30, 2014) (discussing the history of IWF) [hereinafter *IWF History*].

148. The Department of Trade and Industry, a former UK government agency responsible for trade, science, and innovation, has been replaced by agencies, such as the Department of Business, Enterprise, and Regulatory Reform. ISPA is a trade organization comprised of UK Internet Service Providers. The Home Office is a UK government department that oversees immigration, security and drug matters. *See* Keen *supra* note 16, at 366 (explaining the history of the IWF); *IWF History*, *supra* note 148 (describing the multi-stakeholder discussion regarding child pornography on the Internet).

149. The R3 refers to rating, reporting, and responsibility. *See IWF History*, *supra* note 148 (discussing the eventual formation of the IWF).

150. *See* M*emorandum of Understanding Between Crown Prosecution Service ("CPS") and the Association of Chief Police Officers ("ACPO") Concerning Section 46 Sexual Offences Act 2003,* CROWN PROSECUTION SERVICE (Oct. 6, 2004), https://www.cps.gov.uk/publications/docs/mousexoffences.pdf [hereinafter CROWN PROSECUTION SERVICE] (noting the police and CPS' support and partnership with the Internet Watch Foundation in establishing hotlines for individuals to report potentially illegal content); *Vision and Mission*,

combating illegal content on the Internet, specifically child pornography and criminally obscene adult content.[151] The IWF does not initiate its own independent investigations, but rather operates hotlines where members of the public can report child pornography and other illegal content.[152] Once a report is filed, the IWF reviews the legality of the material.[153] Upon a determination that the content violates UK law, the IWF attempts to determine the origin of the material and reports the content to the UK police or an appropriate overseas law enforcement agency.[154] In the United Kingdom, Internet content is regulated pursuant to "offline" regulations.[155] For instance, the IWF reviews reported materials in accordance with laws such as the Sexual Offense Act of 2003—which criminalizes sex crimes, such as rape—and The Protection of Children Act of 1978—which criminalizes the creation and possession child pornography.[156]

With respect to Internet filtering, the IWF's role is limited to compiling a blacklist, labeled the "URL list," from their reports and notifying UK ISPs of illegal content.[157] The list of blocked websites is not made public, however, the IWF maintains that every URL on its

---

INTERNET WATCH FOUND., https://www.iwf.org.uk/about-iwf/remit-vision-and-mission (last visited Dec. 30, 2014) ("Our vision is the elimination of child sexual abuse images online") [hereinafter IWF Mission] .

151. *See* IWF Mission, *supra* note 150 (discussing the organization's goal and mission to fight child pornography on the Internet).

152. See Keen, *supra* note 21, at 366 (describing the IWF reporting process); *see also Report Process*, INTERNET WATCH FOUNDATION, https://www.iwf.org.uk/hotline/report-process (last visited Dec. 30, 2014) (explaining the IWF's reporting process) [hereinafter IWF Reporting Process].

153. *See* CROWN PROSECUTION SERVICE, *supra* note 151 at 6 (discussing the IWF's role);IWF Reporting Process, *supra* note 153 (describing the IWF's reporting process).

154. *See URL List*, INTERNET WATCH FOUND., https://www.iwf.org.uk/members/member-policies/url-list (last visited Dec. 30, 2014) (explaining that the IWF's also notifies their partner organizations in other countries of non-UK sites containing pornography) [hereinafter IWF URL List].

155. *See* Keen, *supra* note 21, at 368-69 (noting that offline laws govern what is suitable on the Internet); *see also Internet Censorship: Law & Policy Around the World*, ELECTRONIC FRONTIERS AUSTRALIA, https://www.efa.org.au/Issues/Censor/cens3.html#uk (last visited Dec. 30, 2014) (noting that as of the time the report was written, the United Kingdom has not enacted censorship legislation specific to the Internet).

156. *See* Sexual Offence Act, 2003, c. 42, sch. 6 (U.K.) The Protection of Children Act, 1978 c. 37 (U.K.); Keen, *supra* note 21, at 366 (discussing that IWF reviews material pursuant to UK "offline" laws); *Laws Relating to the IWF's Remit*, INTERNET WATCH FOUND., https://www.iwf.org.uk/hotline/the-laws (last visited Dec. 30, 2014) (listing the pertinent laws that IWF uses to assess reported material).

157. *See IWF URL List*, *supra* note 154 (discussing the URL list); Keen, *supra* note 78, at 367 (explaining the IWF's blacklist); Open Net Initiate, *supra* note 144, at 360 (discussing the IWF's role of compiling a blacklist of websites).

list depicts indecent images of children or advertisements to illegal content.[158] Aside from informal pressures, currently there is no EU or UK law that requires ISPs to utilize filters.[159] The actual act of blocking results from an ISP's decision to utilize the URL list.[160]

In 2003, The British Telecom ("BT"), one of the largest UK ISPs, designed a new Internet filtering system, dubbed "CleanFeed."[161] CleanFeed is designed to prevent their customers from accessing any illegal content listed on the URL list.[162] While the exact design of BT's CleanFeed has not been published, research has extrapolated the suspected design based.[163] CleanFeed purportedly utilizes a two-tiered hybrid design of traffic redirection and web proxies intended to be extremely precise while maintaining low operation costs and management.[164]

2. Prime Minister's Proposal: Default Filtering for Everyone

In July 2013, UK Prime Minister David Cameron began advocating for the default filtering of pornography, prefacing that

158. *See IWF URL List Recipients*, INTERNET WATCH FOUND., https://www.iwf.org.uk/members/member-policies/url-list/iwf-list-recipients (last visited Dec. 30, 2014) (noting to whom the organization gives their URL list); *see also* Lillian Edwards, *'From Child Porn to China, in One CleanFeed,'* 3(3) SCRIPT-ED, 174 (2006), *available at* http://www.law.ed.ac.uk/ahrc/script-ed/vol3-3/editorial.pdf (noting that the IWF does not release its URL list).

159. *See* ONI UK Report, *supra* note 142, at 359 ("This is consistent with broader EU law which states that ISPs acting as 'mere conduits' of information are not liable for any illegal information transmitted."); Keen, *supra* note 21, at 367 (noting that aside from informal pressures, ISPs are not required to utilize the URL list).

160. *See IWF URL List*, *supra* note 154 (noting that since 2004 many ISPs have chosen to utilize the URL list); *see also* Keen, *supra* note 21, at 367 ("[T]the blocking solution is entirely a matter for the company deploying the list.").

161. *See* Open Net Initiative: United Kingdom, *supra* note 144, at 360 (discussing the filtering system, CleanFeed). *See generally* Richard Clayton, *Failures in a Hybrid Content Blocking System*, https://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf (last visited Dec. 30, 2014) (discussing the flaws of the CleanFeed system).

162. *See* Clayton, *supra* note 161, at 1-2 (explaining the system's design); *see also* Open Net Initiative: United Kingdom, *supra* note 144, at 283 (explaining that BT blocks Web sites that are flagged by IWF).

163. *See* Clayton, *supra* note 162, at 4 (prefacing his report that BT has not disclosed the design of CleanFeed).

164. *See* Clayton, *supra* note 162, at 4 (describing CleanFeed's two-tier design); Richard Clayton, *Anonymity and Traceability in Cyberspace*, CAMBRIDGE UNIV. COMPUTER LABORATORY, TECH. REP. NO. 653, 120-22 (November 2005), *available at* http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-653.pdf (describing that system's advantages).

online pornography is "corroding childhood."[165] The proposed measure will involve preliminary contact from the ISP, asking whether the family would like to activate "family friendly filters" to restrict adult material.[166] Customers who do not select an option will have the filters activated by default.[167] The proposed measures will also affect the UK's Internet access at the infrastructure level.[168] UK ISPs have rewired their infrastructure, affecting all devices connected to a subscriber's home Internet account.[169] The Open Rights Group, an organization defending Internet freedom, spoke with several UK ISPs and discovered that users will also be required to opt-in for any content tagged as violent, extremist, terrorist, anorexia and eating disorders, suicide, alcohol, smoking, Web forums, esoteric material, and Web-blocking circumvention tools.[170]

---

165. Oliver Wright, *David Cameron Cracks Down on Online Pornography With 'Porn Block' Option*, THE INDEP. (July 22, 2013), http://www.independent.co.uk/news/uk/politics/david-cameron-cracks-down-on-online-pornography-with-porn-block-option-8725803.html (reporting that every UK home will have pornography blocked by their Internet provider unless the householder choose to receive it); *see* Ryan Neal, *War On Porn In The UK: Does David Cameron's Plan To Battle Child Pornography Go Too Far?*, INT'L BUS. TIMES (July 22, 2013), http://www.ibtimes.com/war-porn-uk-does-david-camerons-plan-battle-child-pornography-go-too-far-video-1355279 ("By the end of the year, anyone in the UK creating a new broadband account or switching ISPs will have to actively disable filters to access porn.").

166. *See* David Cameron, The Internet and Pornography: Prime Minister Calls for Action, (July 22, 2013), *available at* https://www.gov.uk/government/speeches/the-Internet-and-pornography-prime-minister-calls-for-action (describing the onset of the proposed measure); *see also supra* note 166 and accompanying text (discussing the UK Prime Minister's plan).

167. *See supra* notes 165-66 and accompanying text (describing the process of implementing the new filters).

168. *See supra* notes 165-66 and accompanying text (describing the effect of the new filters).

169. *See* Cameron, *supra* note 166 (discussing that the ISPs have rewired their technology so that once filters are installed they will cover any device connected to home Internet account); Josh Taylor, *UK to Automatically filter 'Adult' Internet Content*, ZDNET (Jul. 23, 2013), http://www.zdnet.com/article/uk-to-automatically-filter-adult-internet-content/ (reporting that the filters can only be deactivated by an account holder, who must be an adult).

170. *See* Ryan Neal, *UK Porn Filter: Censorship Extends Beyond Pornography, But One ISP Is Fighting Back*, INT'L BUS. TIMES (Jul. 26, 2013, 2:59 PM), http://www.ibtimes.com/uk-porn-filter-censorship-extends-beyond-pornography-one-isp-fighting-back-1361379 (reporting leaks that linked the filters to controversial Chinese company, Huawei); *see also* Jim Killock, *Sleepwalking Into Censorship*, OPEN RIGHTS GROUP (Jul. 25, 2013), https://www.openrightsgroup.org/blog/2013/sleepwalking-into-censorship (recommending an alternative to default filtering).

To summarize, the United Kingdom has traditionally operated a libertarian model of Internet governance.[171] Although there is heavy filtering regarding child pornography and illegal content, the filtering is the result of citizen action and reviewed by offline legislation.[172]

3. Intellectual Property Law: United Kingdom

Similar to the United States, the United Kingdom is also a member party of the Berne Convention, the WIPO and the WIPO Treaty.[173] Consequently, the United Kingdom is required to implement legal protection and effective legal remedies against the circumvention of effective technological measures.[174] As a member of the European Union, the United Kingdom has implemented the bloc's directives into their repertoire of intellectual property laws.[175]

The E-Commerce Directive establishes transparency and information requirements for online service providers, and a intermediary liability system.[176] Section 4, Articles 12 to 15 of the Directive establish the framework for intermediary liability in the form of a "notice-and-action" system.[177]

---

171. *See supra* notes 143-47 and accompanying text (describing that the United Kingdom has traditionally operated a libertarian approach in respects to the Internet).

172. *See supra* notes 155-56 and accompanying text (describing the IWF's assessment of reported content in accords to "offline" laws).

173. The United Kingdom ratified the Berne Convention on September 5, 1887. *See WIPO-Administered Treaties*, WORLD INTELL. PROPERTY ORG., http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=15 (last visited Dec. 30, 2014) (providing a list of the members of the Berne Convention). The United Kingdom ratified the WIPO Treaty on December 14, 2009. *See WIPO-Administered Treaties*, WORLD INTELL. PROPERTY ORG., http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=16 (last visited Dec. 30, 2014) (list of WIPO Treaty parties).

174. WIPO Treaty, *supra* note 109, art. 11.

175. The United Kingdom implemented the EU E-Commerce Directive by enacting the Electronic Commerce Regulations of 2002. *See* The Electronic Commerce (EC Directive) Regulations, 2002, S.I. 2001/2555 (U.K.).

176. *See* Directive 2000/31/EC of the European Parliament on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce), 2000 O.J. L 178/1 [hereinafter E-Commerce Directive]; *E-Commerce Directive, Introduction to the Directive*, EUROPEAN COMMISSION, http://ec.europa.eu/internal_market/e-commerce/directive/index_en.htm#maincontentSec1 (last visited Dec. 30, 2014) (providing an overview of the E-Commerce Directive).

177. E-Commerce Directive, *supra* note 177, § 12, art. 12-15; *see Notice-and-Action Procedures*, EUROPEAN COMMISSION, http://ec.europa.eu/internal_market/e-commerce/notice-and-action/index_en.htm (last visited Dec. 30, 2014) (providing an overview of the E-Commerce Directive's notice-and-action procedure).

Pursuant to Article 14 of the E-Commerce Directive, providers that store third party content on their servers may not be held liable for the content unless the service provider fails to expeditiously remove or block access to the content upon obtaining actual knowledge of the content's illegality or upon becoming aware of facts or circumstances that indicate illegal activity.[178] Similar to the criticisms of the DMCA in the United States, there are concerns that the E-Commerce Directive's notice-and-action procedure possibly chills freedom of expression.[179] Critics argue that because service providers risk liability if the content is not expeditiously removed, it is likely that host service providers will systematically take down any alleged unlawful material when a notification is received.[180] Moreover, unlike the DMCA, the E-Commerce Directive does not require Member States to implement "put back" procedures.[181]

Following the footsteps of New Zealand and France, the United Kingdom enacted the Digital Economy Act 2010 ("DEA"), a graduated response law.[182] The DEA establishes the framework of the law, and delegates the implementation and specific details to be later drafted by the Office of Communications ("OFCOM") in an Initial Obligations Code.[183] Under the DEA, once a copyright holder files a copyright infringement report, the ISP is required to notify the reported subscriber to cease the illegal activity and offer the

178. E-Commerce Directive, *supra* note 177, § 12, art. 14 (explaining hosting liability).

179. *See* Rosa Julià-Barceló & Kamiel J. Koelman, *Intermediary Liability In The E-Commerce Directive: So Far So Good, But It's Not Enough,* 16 COMPUTER L. & SECURITY REV. 231, 234-39 (2000) (arguing that the E-Commerce Directive threatens freedom of speech and fair competition); *see also* Pablo Baistrocchi, *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce* 19 SANTA CLARA COMPUTER & HIGH TECH. L.J 111, 130 (2002) (discussing that the loopholes in the directive present an impracticable future).

180. *See* Julià-Barceló & Koelman, *supra* note 179, at 231 (explaining that on-line intermediaries have an incentive to systematically take down material without hearing from the party whose material is removed); *infra* notes 275-92 and accompanying text (discussing similar effects on Internet speech by the DMCA).

181. "Put back" procedures are the processes of putting the alleged infringing material back on the website after going through the statutorily enumerated or court ordered processes. *See* Baistrocchi, *supra* note 180, at 125 (arguing that the E-Commerce Directive should implement "put back" procedures); Julià-Barceló & Koelman, *supra* note 180, at 238-39 (calling for Member States to implement appropriate procedures on notice, take-down and "put back").

182. As the name suggests, a graduated response law incorporates escalating sanctions for repeated offenders. *See* Digital Economy Act, 2010, c. 24 (U.K.) [hereinafter DEA].

183. *See* DEA, §§ 5-6 (U.K.). Sections 5 & 6 of the DEA establishes the process and requirements for approval of the initial obligations code. *See id*. Section 7 establishes the skeleton framework for DEA and leaves the details to OFCOM. *See id*. § 7.

subscriber advice on how to prevent further infractions of the law.[184] Pursuant to § 4, ISPs are required to maintain a list of subscribers who have reached the OFCOM-determined threshold number of infringements.[185] This list must also be provided to copyright holders upon their request.[186] One potentially troubling aspect of the DEA is that repeat offenders risk facing increasing sanctions that may limit or even cut off their Internet connection.[187]

In July 2010, TalkTalk, a UK ISP, joined BT in seeking the judicial review of the DEA, arguing that the act was rushed through parliament before the general election and without proper consideration of its effect on human rights and businesses.[188] On November 10, 2010, the High Court of Justice, the UK court that hears appeals and first instance cases, granted review permission.[189] The High Court ruled in favor of the government on April 20, 2011.[190] High Court Judge Kenneth Parker considered the DEA "a more efficient, focused, and fair system than the current arrangement."[191] On March 6, 2012, TalkTalk and BT lost their final appeal against the implementation of the DEA.[192]

---

184. *See id*. § 3.

185. *See id*. § 4.

186. *See id*.

187. *See id*. § 9; *see also* Robert Andrews, *Digital Economy Bill: A Quick Guide*, THE GUARDIAN, (Apr. 8, 2010), http://www.theguardian.com/media/pda/2010/apr/08/digital-economy-bill-quick-guide-45-measures (discussing the main points of the DEA).

188. *BT and TalkTalk Challenge Digital Economy Act*, BBC (July 8, 2010), http://www.bbc.co.uk/news/10542400 ("The act became law shortly before parliament was dissolved in the so-called wash-up period. It meant it was subject to a shorter debate than other acts"); Josh Halliday, *BT and TalkTalk Granted Judicial Review of Digital Economy Act*, THE GUARDIAN (Nov. 10, 2010, 9:20 AM), http://www.theguardian.com/technology/2010/nov/10/bt-talktalk-digital-economy-act (reporting that both broadband providers was granted review of the act at the high court to clarify whether it conflicts with existing EU legislation).

189. Halliday, *supra* note 189 (reporting that the High Court of Justice granted review permission); *Digital Economy Act to Be Reviewed by Courts and Parliament*, OUT-LAW.COM (Nov. 10, 2010), http://www.out-law.com/page-11538 ("The High Court has said that it will review the law to see if it is in conflict with EU laws on privacy and ISPs' liabilities for users' behaviour.").

190. *See* R v. Sec'y of State for Bus., Innovation and Skills, [2011] EWHC (Admin) 1021 (U.K.); *see also Digital Economy Act Judicial Review*, GOV.UK (Apr. 20, 2011), https://www.gov.uk/government/news/digital-economy-act-judicial-review (reporting that UK Justice Kenneth Parker upheld the principle of taking measures to tackle the unlawful downloading copyright material).

191. R v. Sec'y of State for Business, Innovation and Skills, [2011] EWHC (Admin) 1021, [H9] (U.K.) (holding that the DEA is not disproportionate restriction on right to free expression or to impart and receive information); *see* Andrew Orlowski, *What Now for the Anti-Piracy Law?*, THE REG. (Apr. 21 2011), http://www.theregister.co.uk/2011/04/21/

D. *China: Isolation Behind the Great Firewall*

The Constitution of the People's Republic of China establishes the framework and principles of government and enumerates the rights of Chinese citizens.[193] Article 35 of the Chinese Constitution provides that "[c]itizens of the [PRC] enjoy freedom of speech, of the press, of assembly, of association, of recession and of demonstration."[194] Similar to the United States, China's constitutional protection of freedom of expression is not absolute.[195] The PRC's Constitution expressly limits freedoms that infringe upon the interests of the state, society, or other citizens.[196] Moreover, government regulations further restrict the freedom of speech, such as the Regulations of the People's Republic of China on the Administration of Audio-Visual Products, and the Regulations on Broadcasting and Television Administration, which prohibit the distribution and

digital_economy_act_high_court/ (reporting that High Justice Parker repeatedly disagreed with the objecting ISP's interpretation of the Act).

192. *See* Kelly Fiveash, *BT, TalkTalk Lose Final Appeal Against Digital Economy Act*, THE REG. (Mar. 6, 2012, 10:24 AM), http://www.theregister.co.uk/2012/03/06/bt_talktalk_lose_final_appeal_against_digital_economy_act/ (reporting that Lady Justice Arden, Lord Justice Richards and Lord Justice Patten al upheld the High Court's earlier judgment on all grounds other than on the matter of costs); Josh Halliday, *BT and TalkTalk Lose Challenge Against Digital Economy Act*, THE GUARDIAN (Mar. 6, 2012), http://www.theguardian.com/technology/2012/mar/06/Internet-provider-lose-challenge-digital-economy-act (reporting that the government can begin implementing the Digital Economy Act).

193. *See* Guosong Shao, *The Chinese Legal System, in* INTERNET LAW OF CHINA, 1, 2 (2012) (discussing the background information of the Chinese legal system); *see also* Robert Koeze & Thomas Rimmer, *Constitutional Law,* CHINA GUIDING CASES PROJECT, *available at* http://cgc.law.stanford.edu/english-law-summaries/constitutional-law/ (last visited Dec. 30, 2014) (providing an overview of the PRC's Constitution). *See generally* XIANFA (1982) (China) (enumerating the rights of citizens and establishing the framework for the judicial, legislative and executive branch).

194. XIANFA art. 35 (2004) (China) ("A citizen of the People's Republic of China has right to the freedom of speech, of press, of assembly, of procession and of demonstration."). Since the PRC was found in 1949, the National People's Congress has adopted four constitutions, all of which provided for the protection of the freedom of expression. *See* James Liu, China, ENCYCLOPEDIA BRITANNICA, http://www.britannica.com/EBchecked/topic/111803/China/258953/Constitutional-framework (last visited Apr. 5, 2015) (providing a general overview of China's consitutitonal history).

195. *See* XIANFA art. 51 (2004) (China); Guosong Shao, *Internet Speech, in* INTERNET LAW OF CHINA, 49, 49-53 (2012) [hereinafter Shao, *Internet Speech*] (explaining that the PRC Constitution stipulates that a citizen's exercise of their freedoms and rights may not infringe upon the interest of the state, society, and other citizens).

196. *See* XIANFA art. 51 (2004) (China); Shao, *Internet Speech*, *supra* note 195, at 49-53 (describing the enumerated limitations on speech).

broadcast of matters that endanger the nation's unity and sovereignty, and territorial integrity, respectively.[197]

1. Regulations from the Down Up

The Internet presents the Chinese government with the conundrum of maintaining economic growth provided by the Internet's global reach while preserving its political and ideological control free from international influences.[198] Internet activity in China is regulated through infrastructure and the legal framework, involving various government agencies and criminal or financial sanctions.[199]

The Ministry of Industry and Information Technology ("MIIT") regulates telecommunications, such as the Internet, and oversees telecommunication regulatory agencies in all Chinese provinces, autonomous regions, and municipalities.[200] In addition, similar to the United States, the Internet is regulated by different agencies based on

197. *See* Shao, *Internet Speech*, *supra* note 195, at 53 (detailing the numerous laws and regulations that restrict speech); *see, e.g.*, Yinxiang Zhipin Guanli Tiaoli Shixiao (音像制品管理条例[失效) [Regulations on the Administration of Audio and Video Products] (promulgated by the State Council, Dec. 25, 2001, effective Dec. 7, 2013) (Lawinfochina) (China) (prohibiting the distribution of in audio-visual products that may endanger the "unity and territorial integrity of the nation and sovereignty of the State;"); Guangbo Dianshi Guanli Tiaoli (广播电视管理条例) [Regulations on Broadcasting and Television Administration] (promulgated by the State Council, Aug. 11, 1997, effective Sept. 1, 1997) (Lawinfochina) (China) (prohibiting broadcasting stations from producing or broadcasting content that endangers the unity, sovereignty and territorial integrity of the country); Chuban Guanli Tiaoli (出版管理条例) [Regulations on the Administration of Publication] (promulgated by the State Council, Dec. 25, 2001, effective Feb. 1, 2002) (Lawinfochina) (China) (prohibiting the publication of any content that includes, inter alia, the propagation of evil cults or superstition and content that disturbs public order or public stability).

198. *See* Xiaoru Wang, Behind the Great Firewall: The Internet and Democratization of China (2009) (unpublished Ph.D dissertation, University of Michigan) (on file with University of Michigan Library) (explaining that China's extensive Internet censorship is a result of the government attempting to maintain ideological control); *see also,* Shao, *supra* note 196, at 58-81 (describing China's attempt to restrict Internet speech that may endanger national security and stability).

199. *See* Aaron D. McGeary*, China's Great Balancing Act: Maximizing the Internet's Benefits While Limiting Its Detriments*, 35 Int'l Law. 219, 224-30 (2001) (describing the PRC's efforts to regulate the Internet). *See generally* Guosong Shao, *Regulating the Internet*, *in* INTERNET LAW OF CHINA, 25, 30-44 (2012) [hereinafter Shao, *Regulating the Internet*) (describing the various methods that People's Republic of China employs to regulate the Internet).

200. *See* Shao, *Regulating the Internet*, *supra* note 199, at 31 (explaining that according to PRC Telecommunications Regulations, the Internet is part of the telecommunications business); *see also* Major Responsibilities, CHINESE GOVERNMENT'S OFFICIAL WEB PORTAL, http://www.gov.cn/english//2005-10/02/content_74176.htm (last visited Dec. 30, 2014) (explaining the role of the MIIT).

the specific Internet activity.[201] For instance, China's General Administration of Press and Publication ("GAPP") regulates Internet publishing, and the State Administration of Radio Film and Television ("SARFT") regulates websites providing audio-visual programs.[202]

In addition to the involvement of various agencies, numerous laws regulate behavior and content on the Internet.[203] For instance, unlike the United States and the United Kingdom, the MIIT has established regulations with strict intermediary liability for Internet content providers, bulletin board systems, or other user-generated content sites, for the content published on their sites.[204] Under the National People's Congress ("NPC") Standing Committee's *Decision on Preserving Computer Network Security*, citizens are forbidden from using the Internet to incite secession, divulge state secrets, advocate for the overthrow of state power and the socialist system, provoke ethnic hatred or discrimination, or to propagate violent resistance to law enforcement.[205]

---

201. *See* Shao, *Regulating the Internet*, *supra* note 199, at 31 ((describing the roles of the government agencies); Agencies Responsible for Censorship in China, Congressional-Executive Commission on China, http://www.cecc.gov/agencies-responsible-for-censorship-in-china (last visited Dec. 31, 2014) (detailing the various agencies that are responsible for China's censorship).

202. *See* Shao, *Regulating the Internet*, *supra* note 199, at 31 ((describing the roles of GAPP and SARFT in regards to the internet); Agencies Responsible for Censorship in China, Congressional-Executive Commission on China, http://www.cecc.gov/agencies-responsible-for-censorship-in-china (last visited Dec. 31, 2014) (detailing the various agencies that are responsible for China's censorship).

203. *See infra* notes 204-09 (detailing various laws that regulate the Internet in China).

204. *See* Hulianwang Dianzi Gongao Fuwu Guanli (互联网电子公告服务管理规定) [Management Provisions on Electronic Bulletin Services in Internet] (promulgated by the Ministry of Information and Industry, Nov. 6 2000, effective Nov. 6, 2000) (Lawinfochina) (China) (requiring service providers that find illegal content listed in their system to immediately delete the content, keep relevant records, and report the findings to the authorities); ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 265 (Jonathan Zittrain et al. eds., 2008) (noting that Internet content providers are directly responsible for what is published on their site); *see also Internet Intermediaries*, *supra* note 18, at 7 (explaining that China has adopted a strict intermediary liability approach).

205. Quanguo Rwn Da Chang Weihuì Guanyu Weihu Hulianwang Anquan De Juedìng (全国人大常委会关于维护互联网安全的决定) [Decision of the Standing Committee of the National People's Congress on Preserving Computer Network Security] (promulgated by Standing Committee of the National People's Congress, Dec. 28, 2000, effective Dec. 28, 2000) (Lawinfochina) (China) [hereinafter Decision on Preserving Computer Network Security] (prohibiting specified conduct on the Internet); *see* Shao, *Internet Speech*, *supra* note 195, at 73 (referring to the regulation as the "Decision on Safeguarding Internet Security" as an acceptable alternative translation of the title).

In an effort to protect children and moral values, the PRC further prohibits the production and dissemination of pornographic materials.[206] The *Criminal Law* defines pornography as "materials that explicitly describe sexual conduct or blatantly appeal to the prurient interests."[207] The *Decision on Preserving Computer Network Security* extends the prohibition of pornography to the Internet by criminalizing the establishment of pornographic websites and services.[208] This expansion to the Internet has prompted the Supreme People's Court, the highest court in the PRC, and the Supreme People's Procuratorate, the highest prosecutorial agency, to publish judicial interpretation guidelines in order to clarify the standard for criminal liability, and to delineate the factors for determining whether a website is pornographic.[209]

---

206. China's prohibition of pornography can be traced to the 1979 revision of China's Criminal Law. *See* Shao, *Internet Speech*, *supra* note 195, at 73 (explaining the history of PRC's prohibition of pornography); *see* Ningzhu Zhu, Porn Crackdown Crucial to Cyber Development: Experts, XINHUA NEWS (Apr. 16, 2014), http://news.xinhuanet.com/english/china/2014-04/16/c_133267415.htm (last visited Dec. 31, 2014) ((quoting Han Jun, Deputy Dean of the School of Journalism and Communication at Northwest University) ("[r]ampant pornography has disrupted social order and tainted the image of the country as a whole, casting a bad influence on the public, particularly minors")).

207. Section 9 Article 367 prohibits the production, sale or dissemination of obscene materials, with the exception of scientific products, literary, and artistic works. Zhonghua Renmin Gongheguo Xingfa (97 Xiuding) (**中**华人民共和国刑法 (97**修**订)) [Criminal Law of the People's Republic of China (97 Revision)] (promulgated by National People's Congress, Mar. 14, 1997, effective Oct. 1 1997) (Lawinfochina) (China) [hereinafter Criminal Law].

208. *See* Decision on Preserving Computer Network Security, *supra* note 213, § 3(5) (prohibiting the establishment of pornographic web sites); *see also* Shao, *Internet Speech*, *supra* note 196, at 86-89 (explaining China's attempts to prohibit pornography).

209. The 2010 Interpretation was a revision of the original Supreme People's Courts interpretation issued in 2004. *See* Zuigao Renmin Fayuan, Zuigao Renmin Jianchayuan Guanyu Banli Liyong Hulianwang, Yidong Tongxun Zhongduan, Shengxuntai Zhizuo, Fuzhi, Chuban, Fanmai, Chuanbo Yinhui Dianzi Xinxi Xingshi Anjian Juti Yingyong Falu Ruogan Wentí De Jieshi (**最高人民法院、最高人民**检察院关于办理**利用互**联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释) [Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Concrete Application of Law in the Handling of Criminal Cases of Making, Reproducing, Publishing, Selling and Spreading Pornographic Electronic Information by Means of the Internet, Terminal of Mobile Communications and Sound Message Stations] (promulgated by Supreme People's Court, Supreme People's Procuratorate Feb. 2, 2010, effective Feb. 4, 2010) (Lawinfochina) (China) [hereinafter 2010 Judicial Interpretation] (interpreting the application of the Criminal Law of the People's Republic of China and Decision on Computer Network Security in respect to online pornography).

Furthermore, the PRC prohibits the propagation of cults on the Internet.[210] While the Chinese Constitution provides a right to religion, the People's Supreme Court defines a cult as an illegal organization that hides behind religion, Qigong, or other supernatural beliefs.[211] In addition, the PRC treats cults as organizations that intend to jeopardize public order and social stability.[212] The emergence of the Internet has provided these alleged cults with new avenues to spread their message to a wider audience.[213] For instance, in 1999 the Chinese government banned the Falun Gong, an organization practicing Qigong, an ancient Chinese practice that integrates physical postures, breathing techniques, and meditation.[214] Since then,

---

210. Decision on Preserving Computer Network Security, *supra* note 213, § 2(4) (criminalizing the "use of the computer network to form cult organizations or contact members of cult organizations . . . ."); Article 300 of the Criminal Law prohibits people from using cult organizations or superstitions to undermine law enforcement. Criminal Law, *supra* note 207, art. 300.

211. XINFA art. 36 (stating that no organization or individual may compel citizens to believe in, or not to believe in, any religion). The right to religious practice in China is limited. *See Religious Freedom in China*, BERKLEY CENTER FOR RELIGION, PEACE, AND WORLD AFF. AT GEORGETOWN U., http://berkleycenter.georgetown.edu/essays/religious-freedom-in-china (last visited Dec. 31, 2014) (describing the PRC's regulation of religion within China). The government protects what it calls "normal religious activity," which is restricted to government-sanctioned religious organizations and registered places of worship. *See id*.. Zuigao Renmín Fayuan, Zuigao Renmin Jianchayuan Guanyu Banli Zuzhi He Liyong Xiejiao Zuzhi Fanzuì Anjian Juti Yingyong Falu Ruogan Wentí De Jieshi (**最高人民法院、最高人民**检察院关于办理组织和利用邪教组织犯罪案件具体应用法律若干问题的解释) [Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on the Concrete Application of Law on Handling the Cases of Committing Crimes by Organizing and Using Cult Organizations] (promulgated by Supreme People's Court, Supreme People's Procuratorate, Oct. 9, 1999, effective Oct. 9, 1999) (Lawinfochina) (China) (interpreting the application of the Criminal Law of the People's Republic of China in regards to prosecution of cults and cultists) [hereinafter PRC Cult Regulation]; *see also* Shao, *Internet Speech*, *supra* note 195, at 90 (explaining China's prohibition of cults).

212. *See* PRC Cult Regulation, *supra* note 211 (defining the term cult).

213. *See* James Tong, *An Organizational Analysis of the Falun Gong: Structure, Communications, Financing*, CHINA Q., Sept. 2002, at 639 (discussing how the Internet played a large role in spreading the Falungong's message); *see also* Shao, *Regulating the Internet*, *supra* note 199, at 91 (explaining how Chinese cults have used the Internet to disseminate their views).

214. What distinguishes the Falun Gong from typical Qigong practices is that the Falun Gong has deified their Qigong Master, Li Hongzhi. *See* Christopher Chaney, *The Despotic State Department in Refugee Law: Creating Legal Fictions to Support Falun Gong Asylum Claims*, 6 ASIAN-PAC. L. & POL'Y J. 4 (2005) (discussing the Falun Gong's deification of Li); *see also Who is Li Hongzhi?*, BBC (May 8, 2011) http://news.bbc.co.uk/2/hi/asia-pacific/1223317.stm ("Li Hongzhi, a former trumpet-player from north-east China, is known as 'Living Buddha' to his devotees.").

the Falun Gong has mainly used the Internet to circulate its doctrines, recruit members, and organize activities.[215]

2. Behind the Great Firewall of China

The PRC further exercises extensive control over its internal Internet architecture.[216] Open Net Initiative, a joint project that examines and reports countries' Internet filtering practices, reported that China's filtering has grown continuously more refined, sophisticated, and targeted.[217] China's network is divided into two tiers, the backbone networks and the access networks.[218] The backbone networks run through internationally-leased circuits that connect China to international websites.[219] In the United States and the United Kingdom, a significant percentage of backbone networks are operated and owned by private companies.[220] However, in China, the original four backbone networks are controlled and monitored by various government agencies.[221] Because Internet data enters China

---

215. *See* Shao, *Internet Speech*, *supra* note 195, at 91 (discussing cult's use of the Internet in China); *see also* Tong, *supra* note 214, at 647 (describing the Falun Gong's use of the Internet).

216. *See* Shao, *Regulating the Internet*, *supra* note 199, at 42-46 (2012) (describing how the major telecommunications operations and Internet content providers are required to take measures to prevent the dissemination of illegal information on the Internet); Open Net Initiative, China, OPEN NET INITIATIVE 276-85 *available at* http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-china.pdf (discussing the various technical filtering measures employed by the PRC).

217. *See* Open Net Initiative, China, *supra* note 216, at 276-82 ("Despite the rapid spread of Internet access throughout its vast population, China also has one of the largest and most sophisticated Internet filtering systems in the world."); Lee & Liu, *supra* note 71, at 129 (describing the recent "extraordinary growth" in China's Internet infrastructure).

218. *See* Shao, *Regulating the Internet*, *supra* note 199, at 42 (describing the two-tier system); *see also* Lee & Liu, *supra* note 71, at 133 (noting that while filters have been installed on different layers of China's Internet, it has been constructed primarily at the backbone network).

219. *See Backbone Definition*, COMPUTER HOPE, http://www.computerhope.com/jargon/b/backbone.htm (last visited Dec. 31, 2014) (defining backbone network); *Backbone Definition*, TECHTERMS, http://www.techterms.com/definition/backbone (last visited Dec. 31, 2014) (defining backbone network).

220. *See, e.g.*, Bambauer, *Orwell's Armchair*, *supra* note 10, at 877 (noting that most of the relevant Internet infrastructure in America, such as the network backbone, routers, and access points, are privately owned); Christopher Williams, *ISP Condemns New BT Backbone*, THE REG. (July 1, 2010), http://www.theregister.co.uk/2010/07/01/aa_bt/ (last visited Dec. 30, 2014) (reporting criticisms about BT's backbones unable to handle current demand).

221. *See* Shao, *Regulating the Internet*, *supra* note 199, at 42 (discussing several of backbone networks in China); *China Mobile Users 2012*, ONBILE (Jan. 25, 2013), http://www.onbile.com/info/china-mobile-users-2012/ (discussing that individuals and businesses are only allowed to rent bandwidth from state networks).

through a limited set of entry points controlled by governmental agencies, the Chinese government is able to regulate the flow of information by controlling these entry points.[222]

China's backbone-level filtering system, officially designated the "Golden Shield Project" (金盾工程) is commonly referred to as the "Great Firewall of China," a reference to the Great Wall of China.[223] Unlike typical firewall systems, however, the Great Firewall of China forms a "virtual ring around an entire country."[224] The second tier of China's network systems, the access networks, is a system of intermediate networks that connect through the backbone networks to the international Internet.[225] All of China's access networks are required to implement technical measures to prevent the dissemination of illegal and harmful information in cyberspace.[226] For instance, access networks are required to record a customer's account number, phone numbers, and IP address.[227]

It is clear that maintaining national security and social stability are some of the PRC's utmost important objectives.[228] By regulating the Internet from the ground up, the PRC is able to control the data that enters and leaves its borders at the infrastructure level while maintaining compliance from its end-user citizens with their broad

---

222. *See* Kristen Farrell, *The Big Mamas Are Watching: China's Censorship of the Internet and the Strain on Freedom of Expression*, 15 MICH. ST. J. INT'L L. 577, 585-86 (2007) (noting that the MIIT ensures that government control exists at every juncture); Lee & Liu, *supra* note 71, at 133 (discussing PRC's attempts to control the limited Internet connection points).

223. Similar to the Great Wall's purpose to defend against marauding invaders, the Great Firewall denotes China's attempt to block undesirable content from its "netizens." *See* Lee & Liu, *supra* note 70, at 133 (describing the firewall project); Jennifer Shyu, *Speak No Evil: Circumventing Chinese Censorship,* 45 SAN DIEGO L. REV. 211, 225-28 (2008)] (describing the goals of the firewall project); s*ee also* Bambauer, *Orwell's Armchair*, *supra* note 10, at 876 (discussing PRC's implementation of filters at access point).

224. *See* Lee & Liu, *supra* note 70, at 133 (describing the firewall's pervasive filtering); Shao, *Regulating the Internet*, *supra* note 199, at 43 (explaining the different ways the Golden Shield Project can block information).

225. *See* Lee & Liu, *supra* note 71, at 133 (describing that the lower layer networks connect through the upper layer networks to the international networks); Shao, *Regulating the Internet*, *supra* note 199, at 42 (describing how China's Internet is divided into two tiers)

226. *See supra* notes 223-25 (explaining the technical measures utilized at the backbone level); *infra* note 227 (explaining the measures implemented at access networks).

227. *See* Farrell, *supra* note 222, at 586 (explaining that Internet Access Points must record a customer's account number, phone number and IP address); Open Net Initiative, China, *supra* note 16, at 284 (noting that Internet Information Service providers are required to store records for 60 days and provide records to authorities upon demand).

228. *See supra* notes 206-15 and accompanying text (describing China's attempt to regulate the Internet in furtherance of maintaining "social stability," and "national security").

censorship laws.[229] China's model of Internet censorship is evocative of Lawrence Lessig's "code-is-law," which provides that "code"—*i.e.*, software or hardware—can have a similar effect to the way legal regulation affects one's behavior.[230] Professor Lee and Professor Liu posit that, "one of the most profound consequences of [China's Internet] architecture is not that it immediately limits citizens' access to sensitive foreign content, but that it is gradually shaping human behavior in cyberspace."[231]

It is clear that the censorship policies of the United States, United Kingdom, and China embody different philosophies and values.[232] For instance, while each country appears to agree on protecting children from inappropriate material, such as pornography, each country approaches the problem differently.[233] The United States regulates the Internet through legislative attempts.[234] The United Kingdom passively designates a watchdog role to a nongovernment organization.[235] China attempts to exercise near-complete domination over the Internet activity within its borders.[236]

II. *ARTICLE 19 ANALYSIS*

Part II of this Note analyzes each country's Internet censorship model under Article 19 of the ICCPR. Section A will analyze the US legislative approach, specifically the possible conflicts of the Digital Millennium Copyright Act with Article 19. Section B examines

---

229. *See supra* notes 199-227 and accompanying text (explaining China's holistic approach to Internet censorship).

230. *See* Lawrence Lessig, CODE: AND OTHER LAWS OF CYBERSPACE, VERSION 2.0 5 (2006) (discussing how code regulates behavior on cyberspace); *see also* Lee & Liu, *supra* note 70, at 26 (utilizing Lessig's theory, Professors Lee and Professor Liu analyzes China's censorship scheme's effect on its citizen).

231. Professor Jyh-An Lee is an Assistant Professor of Law at National Chengchi University, Taiwan. Professor Ching-Yi Liu is a Professor of Law at National Taiwan University, Taiwan. *See* Lee & Liu, *supra* note 70, at 145.

232. *Compare supra* notes 77-141 (discussing the United States' legislative model), *with supra* notes 142-192 (discussing the United Kingdom's approach to Internet regulations), *and supra* notes 199-227 (detailing the PRC's control over their internal Internet activities).

233. *Compare supra* notes 79-106 (discussing CDA, COPA, and CIPA), *with supra* notes 151-65 (discussing the role of the IWF), *and supra* notes 207-10 (detailing the PRC's prohibition of pornography).

234. *See supra* notes 79-141 (describing the various legislative attempts to censor Internet content).

235. *See supra* notes 147-67 (discussing the United Kingdom's support of the IWF).

236. *See supra* notes 199-227 (explaining the PRC's extensive control of internal Internet use).

Article 19's compatibility with the United Kingdom's cooperation with the Internet Watch Foundation, and the United Kingdom's recent adoption of the Digital Economy Act. Finally, as the PRC has not ratified the ICCPR, Section C will look at the *potential* Article 19 violations committed by the PRC's extensive manipulation and regulation of the Internet. As expected, no nation has a perfect model of Internet censorship. This analysis will, however, provide a better understanding of the strengths and possible deficiencies of applying Article 19 to the Internet.

Whether a restriction is considered permissible inevitably evokes a struggle among respect of state sovereignty, cultural and moral differences, and promotion of individual human rights.[237] This struggle is evident in *Hertzberg v. Finland*, in which the HRC could not find an Article 19 violation in a Finnish broadcaster's decision to censor two programs involving homosexuality. [238] The HRC noted that public morals differ widely between countries and that there is no universally common standard of morality.[239] Therefore, "a certain margin of discretion must be accorded to the responsible national authorities."[240] Despite the lack of success after *Hertzberg*, State parties have continued to argue for a "margin of discretion" in HRC cases.[241]

The Internet is arguably unlike any of its predecessors, and the vast potential and benefits of the Internet are the result of its unique characteristics, such as its unparalleled speed, ubiquity, and relative

---

237. *See* Human Rights Comm., Commc'n No. 61/1979, Leo Hertzberg et al. v. Finland, U.N. Doc. CCPR/C/OP/1 (1985) [hereinafter Human Rights Comm., Hertzberg Commc'n] (holding that public morals differ); Carlson, *supra* note 26, at 122-23 (explaining that application of Article 19(3) is uneven).

238. *See* Human Rights Comm., Hertzberg Commc'n, *supra* note 239, ¶ 2.1.

239. *See* Human Rights Comm., Hertzberg Commc'n, *supra* note 238, ¶ 10.3; *see also* Ambika Kumar, *Using Courts to Enforce the Free Speech Provisions of the International Covenant on Civil and Political Rights*, 7 CHI. J. INT'L L. 351, 353 (2006) (discussing how the Human Rights Committee has adjudicated Article 19 matters inconsistently); Carlson, *supra* note 18, at 122 (explaining the significance of Hertzberg).

240. Human Rights Comm., Hertzberg Commc'n, *supra* note 238, ¶ 10.3.

241. *See* Andrew Legg, THE MARGIN OF APPRECIATION IN INTERNATIONAL HUMAN RIGHTS LAW 131 (2012) (stating that states have continued to make the case for deference before the HRC)). *But see* SARAH JOSEPH & JENNY SCHULTZ, et al., THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS 527 (2d ed. 2004) (describing that after Hertzberg, the HRC has never disposed any other Article 19 case by reference to the State Party's "margin of discretion"); *but see also* Human Rights Comm., Commc'n No. 511/1992, Länsman et al. v. Finland, U.N. Doc. CCPR/C/52/D/511/1992 (1994) (unwilling to assess an Article 27 violation by reference to a margin of appreciation).

anonymity.[242] The Special Rapporteur recognized that due to their very nature, many regulations or restrictions that may be legitimate and proportionate for traditional media, such as defamation laws, are often not as effective with regards to the Internet.[243]

While governments typically agree that Internet content should be regulated, their norms justifying filtering differ widely.[244] For instance, people from the United States would likely disapprove of Saudi Arabia's pervasive filtering predicated on Shari'ah law.[245] However, Saudi Arabian residents might similarly object to US tolerance of pornography and alcohol consumption.[246]

Even among democratic countries, justifications for content-restriction diverge.[247] This contrast in norms is evident in the case *Ligue Contre le Racisme et l'Antisémitisme v. Yahoo!, Inc*.[248] In 2000, Yahoo! operated a United States-based auction page, targeted towards Americans, that posted Nazi memorabilia for auction.[249] However, the French Criminal Code prohibits the sale of Nazi memorabilia.[250] Article R645-1 criminalizes the display of uniforms, insignias, or emblems that are associated with "organizations responsible for crimes against humanity," which are not being used for the purposes of a movie, show, or historical pageant.[251] Because anyone from

242. *See The Internet: Challenges, Opportunities and Prospects*, INT'L TELECOMM. UNION (May 17, 2001), http://www.itu.int/newsarchive/wtd/2001/ExecutiveSummary.html (reporting on the prospective benefits of the Internet); August 2011 La Rue Report, *supra* note 52, at 5 (noting the unprecedented level of communication provided by the Internet).

243. The Special Rapporteur used the example of defamation of an individual's reputation. *See* May 2011 La Rue Report, *supra* note 52, at 8. ("[G]iven the ability of the individual concerned to exercise his/her right of reply instantly to restore the harm caused, the types of sanctions that are applied to offline defamation may be unnecessary or disproportionate.").

244. *See infra* notes 246-47 (providing an example of justifications for Internet regulations based on different cultural norms).

245. *See* Internet Rules, 2001, Council of Ministers Resolution (Feb. 12, 2001), (Saudi Arabia) *available at* http://www.al-bab.com/media/docs/saudi.htm (last visited Dec. 30, 2014) (proscribing specific Internet activities and content) [hereinafter Saudi Internet Rules]; *Internet Filtering in Saudi Arabia*, OPENNET INITIATIVE, https://opennet.net/sites/opennet.net/files/ONI_SaudiArabia_2009.pdf (last visited Dec. 31, 2014) (reporting the extent of Internet filtering in Saudi Arabia).

246. *See supra* Part I.B (discussing the United States' model of Internet regulation).

247. *See infra* notes 248-54 (discussing the controversy in Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme, 433 F.3d 1199, 1201 (9th Cir. 2006)).

248. *See* Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme, 433 F.3d 1199, 1201 (9th Cir. 2006) (providing the background of the French Superior Court case).

249. *See id.* at 1202.

250. *See* CODE PÉNAL [C. PÉN.] art. R645-1 (Fr.).

251. *Id.*

France can visit the Yahoo! auction, the plaintiffs, the League Against Racism and Anti-Semitism, argued that Yahoo! was in violation of Article R645-1 of the French Penal Code.[252]

Upon finding that Yahoo! Inc. had violated the Article R645-1, the Superior Court of Paris ordered Yahoo! Inc. to take measures that would prevent French Internet users from receiving Nazi content.[253] While Yahoo! France, Yahoo! Inc.'s French subsidiary, was quick to follow the French Court's order, Yahoo! Inc.'s US office resisted the French order and filed suit in US District Court for the Northern District of California seeking a declaratory judgment that the French Court Order was unenforceable in the United States.[254] This case illustrates the possible conflicts produced by divergent norms and laws, and the Internet's border-defying nature.[255]

There are currently a variety of theories on the government's role vis-à-vis the Internet.[256] For instance, cyber-libertarians, such as John Perry Barlow, argue that access to content on the Internet should remain unfettered.[257] Other scholars, such as Thomas Schultz, espouse a Helgian-model, arguing that sovereign nations must safeguard local values through filtering mechanisms.[258] Recognizing the deficiencies in current theoretical approaches to Internet filtering, Professor Bambauer proposes that censorship practices should be evaluated

252. *See Yahoo! Inc.*, 433 F.3d at 1202 (discussing LICRA's cease and desist letter to Yahoo!, Inc).

253. *See id.* at 1202.

254. *See id.* at 1224 (holding that action was subject to dismissal because the issue was unripe).

255. *See supra* notes 248-54 (discussing the conflict between the countries' differing norms of freedom of expression).

256. *See infra* notes 257-59 (describing different views regarding the government's role vis-à-vis the Internet).

257. In his 1996 work, *A Declaration of the Independence of Cyberspace*, John Perry Barlow prophetically conveys the current struggles governments encounter with regulating the Internet. John Perry Barlow, *A Declaration of the Independence of Cyberspace* (1996), http://homes.eff.org/~barlow/Declaration-Final.html ("Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here."); *see also* Philip Elmer-Dewitt, *First Nation in Cyberspace*, TIME, Dec. 6, 1993, at 62 (quoting John Gilmore) ("The Net interprets censorship as damage and routes around it.")).

258. *See* Thomas Schultz, *Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface*, 19 EUR. J. INT'L L. 799, 806-10 (2008) (proposing a social-contract justification for filtering the Internet).

along the process-based metric of openness, transparency, narrowness, and accountability.[259]

A. *Article 19 Analysis of the United States: What to do with the DMCA?*

The cumulative test of Article 19(3) encompasses principles of predictability and transparency.[260] Openness and transparency of government are often considered key pillars of a democratic society.[261] In a 2009 memorandum, President Obama instructed the head of executive agencies to focus on three principles of an open government: (1) transparency, (2) participation, and (3) collaboration.[262] The memo requires, among other things, executive departments and agencies to: publish government information online; improve the quality of government information; create an environment conducive to transparency, participation, and collaboration on ongoing projects; and reform policy framework to realize the potential of technology.[263]

US laws regarding Internet governance, whether through cases or regulations, are readily available to the public.[264] The effects of

---

259. *See* Bambauer, *Cybersieves*, *supra* note 21, at 390-410 (2009) (establishing a framework for analyzing the legitimacy of a country's censorship system); Bambauer, *Orwell's Armchair*, *supra* note 10, at 900-43 (utilizing the framework to examine the legitimacy of soft censorship systems).

260. *See* Land, *supra* note 48, at 426 (explaining Article 19(3) restrictions); May 2011 La Rue Report, *supra* note 53, at 8 (explaining the three-part cumulative test).

261. *See* JON GANT AND NICOLE TURNER-LEE, GOVERNMENT TRANSPARENCY: SIX STRATEGIES FOR MORE OPEN AND PARTICIPATORY GOVERNMENT, 13-15 (2011) ("A core pillar of democratic society is the interaction between government and the governed."); *cf.* August 2011 La Rue Report, *supra* note 52, at 6 (reporting that the Internet can primarily be used as a positive tool to increase transparency over the conduct of those in power, access diverse sources of information, facilitate active citizen participation in building democratic societies).

262. *See* Memorandum from the Office of Mgmt and Budget on Open Gov't Directive to the Head Executive Dep'ts and Agencies (Dec. 8, 2009), *available at* https:// www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf ("The three principles of transparency, participation, and collaboration form the cornerstone of an open government) [hereinafter Open Directive]; Memorandum from the Office of Press Sec'y on Transparency and Open Gov't to the Head Executive Dep'ts and Agencies (Jan. 21, 2009), *available at* http://www2.gwu.edu/~nsarchiv/news/20090121/2009_transparency_memo.pdf (directing the Chief of the Office of Management and Budget to coordinate with Executive agencies to implement the Open Directive).

263. *See* Open Directive, *supra* note 263, at 2-8 (establishing the plans to implement the Open Directive).

264. There have been numerous Acts passed to increase government transparency. For instance, the Freedom of Information Act and its amendments, allows full or partial disclosure

these laws on speech, however, are not always apparent. In 2010, Google launched its Transparency Report to "provide hard evidence of how laws and policies affect access to information online."[265] Utilizing Google's Transparency Reports, the Electronic Frontier Foundation ("EFF") compiled a list of takedowns that appear to involve possible misuse of the DMCA.[266] The EFF's findings are indicative of scholars' apprehension of DMCA § 512.[267]

The latter aspects of Article 19(3) involve principles of legitimacy, necessity, and proportionality. Attempts at "hard censorship" in the United States are often met with constitutional scrutiny. Recent landmark cases on Internet censorship demonstrate that the courts look to the proportionality of the regulation vis-à-vis the government interest and the legitimacy of the interest.[268] Content-based regulations are often strictly scrutinized.[269] In order for the regulation to survive, the government must show that the limitation serves a compelling state interest and that the means employed are necessary and narrowly tailored to achieve that interest.[270]

Restrictions on speech may not be overbroad.[271] In *Reno*, Justice Steven's opinion noted that the government failed to state why a less

---

of previously unreleased government information and documents. *See* 5 U.S.C.A. § 552 (2009). Moreover, the United States codifies its statutes and regularly publishes its courts opinions.

265. *See* TRANSPARENCY REPORT, GOOGLE, http://www.google.com/transparencyreport/ (last visited Dec. 30, 2014) (providing reports about takedown requests that Google receives).

266. *See* Parker Higgins, *Top 10 Takedowns in Google's Copyright Transparency Report*, Electronic Frontier Found. (July 5, 2012), https://www.eff.org/deeplinks/2012/07/top-10-takedowns-googles-copyright-transparency-report (noting that these dubious takedown show that the DMCA's notice-and-takedown procedures are ripe for abuse).

267. *See infra* notes 275-92 (examining the indirect chilling effects caused by § 512).

268. *See supra* notes 80-94 (examining United States Supreme Court cases involving CDA §223 and COPA).

269. *See* Rosenberger v. Rector & Visitors of Univ. of Virginia, 515 U.S. 819, 829 (1995) (noting that the government must abstain from regulating speech when "the specific motivating ideology or the opinion or perspective of the speaker is the rationale for the restriction.").

270. *See, e.g.*, ACLU v. Reno, 31 F. Supp. 2d 473, 495 (E.D. Pa. 1999) *aff'd*, 217 F.3d 162 (3d Cir. 2000) *vacated sub nom.*, Ashcroft v. ACLU, 535 U.S. 564 (2002) (explaining that the government may regulate the content of such protected speech to promote a compelling governmental interest if the government chooses the least restrictive means to further the articulated interest).

271. *See* UN General Comment 34, *supra* note 50, at 8 ("Restrictions must not be overbroad."); August 2011 La Rue, *supra* note 52, at 6 (discussing that any restrictions must be formulated with specific precision).

restrictive provision would not be as effective as the CDA.[272] Similarly, in *Ashcroft*, Justice Kennedy's concurrence suggested that COPA was likely overbroad and would not survive a constitutional challenge since content-based regulations like COPA are presumptively invalid abridgments of speech.[273] US First Amendment jurisprudence remains a safeguard against government attempts at hard censorship.

While the US Constitution constrains legislative attempts at hard censorship, soft censorship schemes, such as the DMCA, continue to evade constitutional scrutiny.[274] Although the DMCA does not expressly limit freedom of expression, the chilling effect is apparent.[275] Recognizing an intermediary's inclination to err on the side of safety by over-censoring, Special Rapporteur La Rue advised that intermediaries may not be in the best position to make determinations of the legality of particular content.[276] This determination requires careful balancing of competing interests and consideration of defenses.[277] In a 2011 Joint Declaration, the Special Rapporteurs declared, "intermediaries should not be required to monitor user-generated content" and should not be subject to

---

272. Reno v. ACLU, 521 U.S. 844, 879 (1997) (Stevens, J., concurring) ("The breadth of this content-based restriction of speech imposes an especially heavy burden on the Government to explain why a less restrictive provision would not be as effective as the CDA. It has not done so.").

273. Ashcroft v. ACLU, 535 U.S. 564, 591 (2002) ("There is a very real likelihood that the . . . [COPA] is overbroad and cannot survive such a challenge. Indeed, content-based regulations like this one are presumptively invalid abridgments of the freedom of speech.").

274. *See* Bambauer, *Orwell's Armchair*, *supra* note 10, at 890 (arguing that content restrictions via the spending power generally enables the soft censorship to survive First Amendment scrutiny); Seltzer, *supra* note 116, at 176 (arguing that the indirect nature of the chill on speech should not shield the DMCA from challenge).

275. *See infra* notes 283-92 (describing the chilling effects caused by § 512).

276. *See* May 2011 La Rue Report, *supra* note 52, at 12 (arguing that the lack of transparency in the intermediaries' decision-making process obscures discriminatory practices or political pressure affecting the companies' decisions); *cf.* Seltzer, *supra* note 117, at 181 (noting that because the service provider does not share all the benefits of the poster, the service provider lacks a similarly strong incentive to take risks in defending posted material in the face of a complaint).

277. *See* May 2011 La Rue Report, *supra* note 52, at 12 (arguing that intermediaries may not be in the best position to balance competing interests and consideration of defenses); Seltzer, *supra* note 116, at 229 (arguing for an alternative approach that limits takedowns to claimed commercial appropriation of entire works and requires proof to be submitted along with the notification).

extrajudicial takedowns which fail to provide sufficient protection for freedom of expression.[278]

It is debatable whether the current DMCA counter-notification process provides sufficient protection for freedom of expression.[279] Despite its purpose to protect copyrights, some critics argue that the DMCA's "notice-and-takedown" regime has a chilling effect on freedom of expression.[280] For example, the report of suspected terrorist organizations using DMCA takedowns of YouTube videos critical of Islam in efforts to obtain the uploader's name and address is troubling.[281] One critic notes that the notice-and-takedown regime shares many of the hallmarks of prior restraints on speech because the notice-and-takedowns are imposed to limit speech before any formal adjudication on the merits of the copyright claims.[282]

Because of the relatively low costs to claimants and the expectation of prompt takedowns, the DMCA is susceptible to abusive claims.[283] Moreover, because private parties, such as service providers, remove the content, the DMCA evades the level of scrutiny typically evoked by government intervention.[284] Professor Seltzer

---

278. *See* Special Rapporteur on Freedom of Opinion and Expression et al., *Joint Declaration on Freedom of Expression and the Internet*, § 2b, *available a*t http://www.osce.org/fom/78309 (June 1, 2011) [hereinafter *Joint Declaration*].

279. Some other notice-and-action systems, such as the E-Commerce Directive, do not include counter-notifications. *See supra* notes 176-81 (describing the E-Commerce notice-and-action procedure).

280. *See* Seltzer, *supra* note 117, at 116 (arguing that the DMCA's indirect chilling effect upon speech affects the public no less than if the government wrongly ordered the removal of lawful online material directly); John William Nelson, *DMCA Takedowns Versus Free Speech*, LEX TECHNOLOGIAE (October 18, 2010) http://www.lextechnologiae.com/2010/10/18/dmca-takedowns-versus-free-speech/ (discussing how legitimate works can be brought down by illegitimate DMCA take-down notices because service providers are likely to be risk-averse).

281. *See* Doble, *supra* note 120 (reporting the suspected use of DMCA takedowns by terrorist organizations); Tamburro, *supra* note 120 (reporting that a Youtuber is hiding from suspected terrorists after sharing his information pursuant to the DMCA counter-notification procedures).

282. *See* Nelson, *supra* note 281 (arguing that the DMCA framework of prior restraint is inconsistent with the United States' notion of free expression); Seltzer, *supra* note 116, at 190 (arguing for greater constitutional scrutiny of the DMCA because it operates as a prior restraint on expression). *See generally Internet Intermediaries*, *supra* note 18 (recommending improvements to the current notice-and-takedown regime).

283. *See* Seltzer, *supra* note 116, at 178 ("Compounding the problem, the promise of rapid takedown creates an incentive for copyright claimants to file dubious takedown claims"); Urban & Quilter, *supra* note 116, at 624 (2006) (revealing a high incidence of questionable uses of the § 512 process).

284. *See* Mike Masnick, *Why The DMCA Is An Unconstitutional Restriction On Free Speech*, TECHDIRT (Apr. 6, 2010), https://www.techdirt.com/articles/20100402/

notes that the DMCA offers service providers the one-sided choice of either potentially costly, case-by-case risk analysis of defending each claim or streamlined self-censorship.[285] She posits that a rational, risk-averse entity would likely choose the latter, especially since potentially only a third party's speech is at stake.[286] This risk-aversion may surrender valuable speech in the process.[287]

In an effort to study § 512 of the DMCA's effect on the First Amendment, a consortium of law school clinics and the EFF began the "Chilling Effects Project."[288] Beginning in January 2002, the project collected cease-and-desist letters on a "variety of intellectual property and other online-speech-related doctrines such as defamation."[289] Their study revealed takedowns occurring in numerous questionable situations.[290] For instance, a number of notices addressed non-copyright issues, such as a competitor's search engine ranking, trademark rights, or personal privacy.[291] The researchers determined from their limited data that the effect on Internet speech

---

1856128861.shtml (arguing that the DMCA violates the First Amendment); Seltzer, *supra* note 116, at 175-76 (arguing for greater constitutional scrutiny of § 512 because its "indirect chilling effect upon speech harms the public no less than if the government wrongly ordered the removal of lawful online material directly.").

285. *See* Seltzer, *supra* note 116, at 175 (arguing that the DMCA incentivizes streamline censorship).

286. *See id*.

287. *See* May 2011 La Rue Report, *supra* note 52, at 12 (noting intermediaries' inclination to err on the side of safety by over-censoring potentially illegal content); Seltzer, *supra* note 116, at 184 (arguing that the market fails to correct this error because a significant amount of Internet speech is non-commercial and hosted on free or low-margin hosting services).

288. *See* Urban & Quilter, *supra* note 15, at 641; CHILLING EFFECTS http://www.chillingeffects.org (last visited Dec. 30, 2014) [hereinafter CHILLING EFFECTS PROJECT] (describing the goals of the organization, which is to educate people about the protections that the First Amendment and intellectual property laws give to your online activities).

289. *See* Urban & Quilter, *supra* note 115, at 641. Their data set included 876 notices submitted to Chilling Effects over a three year period; see also *About U*s, CHILLING EFFECTS, (last visited Apr. 5, 2015), https://www.chillingeffects.org/pages/about (discussing the aims of the project).

290. *See* Urban & Quilter, *supra* note 115, at 681 (finding a surprisingly large number of notices that present serious substantive questions about the underlying claim); see also *About U*s, CHILLING EFFECTS, (last visited Apr. 5, 2015), https://www.chillingeffects.org/pages/about (discussing that many notices are without merit).

291. *See* Urban & Quilter, *supra* note 115, at 681 (finding the data quite troubling, since the legislative history of § 512 were limited to questions of copyright infringement); *see also* CHILLING EFFECTS http://www.chillingeffects.org (last visited Dec. 30, 2014) (containing a database of improper takedown complaints, including notices based on trademarks).

from processes that lack the traditional safeguards of court proceedings is rather significant.[292]

B. *Article 19 Analysis of the United Kingdom: Who Watches the Watchdogs?*

Special Rapporteur Frank La Rue recognized that an organization that is independent of any unwarranted influence may undertake assessment of blocking sites as long as the entity provides full details regarding the necessity and justification for the censorship.[293] Because the IWF does not directly censor content, however, it is unclear based on the language of Article 19 whether the three-part cumulative test applies to the UK government's cooperation with the IWF because the IWF does not promulgate laws or regulations, and the three-part cumulative test appears to apply only to laws.[294] Because the IWF's "URL list" affects over 95% of UK Internet users, transparency and accountability are essential from that institution.[295] Not only is the IWF's "URL list" confidential, but the IWF also does not publish its findings from its independent review process.[296] A party that receives a notice to takedown or discovers that its site has been added to the "URL list" may appeal the IWF's assessment to the internal appeal board.[297] Because the IWF is

---

292. *See* Urban & Quilter, *supra* note 115, at 682 (arguing that the removal of speech from the Internet without traditional forms of due process is troubling); *see also* Brief of Amicus Curiae for Plaintiff-Appellant at 26, *Perfect 10, Inc. v. Google, Inc*., 653 F.3d 976 (9th Cir. 2011) (No. 10-56316) (referencing the symposium's findings).

293. *See* May 2011 La Rue Report, *supra* note 52, at 20 (calling for increased transparency in filtering); August 2011 La Rue Report, *supra* note 51 at 13 (discussing the possibility of independent organizations in determining what material should be blocked).

294. *See* May 2011 La Rue Report, *supra* note 52, at 8 (stating that any limitation to the right to freedom of expression must be provided by *law*, which is clear and accessible to everyone); August 2011 La Rue Report, *supra* note 51, at 22 (emphasis added) ("Any such *laws* must comply with the three criteria of restrictions . . . .").

295. *See* Dawn C. Nunziato, *The Beginning of the End of Internet Freedom*, 45 Geo. J. Int'l L. 383, 389 (2014) (noting that the United Kingdom has implemented a nationwide filtering system that affects over 98% of Internet subscribers in the country); CJ Davies, *The Hidden Censors of the Internet*, WIRED UK (May 20, 2009), http://www.wired.co.uk/magazine/archive/2009/06/features/the-hidden-censors-of-the-Internet/viewall (reporting that reach of the IWF's blacklist on UK Internet subscribers.)

296. *See* Edwards, *supra* note 159 (noting that the IWF does not publish its URL list).

297. *See Content Assessment Appeal* Process, INTERNET WATCH FOUND., https://www.iwf.org.uk/accountability/complaints/content-assessment-appeal-process (last visited Dec. 31, 2014) (describing IWF's internal appeal process); *Content Assessment Appeal Process: Chart*, INTERNET WATCH FOUND., https://www.iwf.org.uk/assets/media/

a non-government organization, however, there is no judicial appeal of the determinations made within the organization.[298]

The IWF's "URL list," at least facially, does not create a freedom of expression concern because the organization ostensibly only compiles a blacklist of criminal content, such as child pornography. Moreover, the Special Rapporteur underscores that there is a difference between blocking illegal content, which States parties are required to prohibit under international law, and content that may be considered harmful, but of which State parties are neither required to prohibit nor criminalize.[299] However, despite the IWF's limited involvement in the actual censoring of illegal content, the UK filtering system essentially grants the ultimate authority over Internet content to this unaccountable, nontransparent organization.[300]

The 2008 "IWF and Wikipedia" controversy demonstrated the possible over-inclusive censorship resulting from major UK ISPs utilizing the IWF's "URL list."[301] On December 5, 2008, the IWF added Wikipedia URLs for "Virgin Killer," the 1976 album by German heavy metal band Scorpions, to their blacklist.[302] The thirty-

---

accountability/Content%20assessment%20appeal%20process.pdf (flowchart of IWF appeal process).

298. *See* Lord Macdonald of River Glaven, *A Human Rights Audit of the Internet Watch Foundation*, https://www.iwf.org.uk/assets/media/accountability/Human_Rights_Audit_web.pdf (last visited Dec. 30, 2014) (recommending that, based on the rationale in the split decision of the United Kingdom Supreme Court case *YL v. Birmingham City Council*, IWF's assessments should be susceptible to judicial review); *see also* Davies, *supra* note 95 (describing IWF's opaque internal appeals process).

299. *See* August 2011 La Rue Report, *supra* note 51, at 7 (differentiating content that must be prohibited by international law and permissible content). *See generally* Convention on the Rights of the Child, Protocol on the Sale of Children, Child Prostitution and Child Pornography, art. 3(c), *opened for signature* May 24, 2000, 2171 U.N.T.S. 227 (requiring State Parties to criminalize the production and dissemination of child pornography).

300. Because UK's largest ISPs utilize the IWF's URL list, the effect of the blacklist is experienced throughout the nation. *See IWF URL List Recipients*, *supra* note 158 (providing a list of ISPs and telecommunications companies that utilize the URL list); Davies, *supra* note 296 (reporting that Internet content in the United Kingdom is checked against a mysterious, secret blacklist).

301. *See* Davies, *supra* note 295 (reporting on the Wikipedia controversy); *see also infra* notes 302-09 (explaining the over-censorship of Wikipedia that resulted from the IWF's URL list).

302. *See* Frank Fisher, *A Nasty Sting in the Censors' Tail*, THE GUARDIAN (Dec. 9, 2008), http://www.theguardian.com/commentisfree/2008/dec/09/scorpions-virgin-killer-censorship (reporting the controversy over the thirty-year-old album cover); Gordon MacMillan, *Wikipedia Page Banned in UK Over Controversial Child Image*, BRAND REPUBLIC (Dec. 9, 2008), http://www.brandrepublic.com/news/868067/Wikipedia-page-banned-UK-controversial-child-image/ ("An Internet watchdog in the UK has taken the

two-year-old album cover depicted a nude prepubescent girl.[303] The IWF justified the inclusion of the sites that showed the album cover because the cover contained "potentially illegal child sexual abuse image."[304] However, as a result of the block, UK users were unable to view the page or edit the Wikipedia article, consequently preventing them from removing the picture.[305] ISPs utilizing the "URL list" would re-route Wikipedia traffic through a proxy server, resulting in Wikipedia being unable to distinguish UK users from one another by their IP addresses.[306] This influx from a single source triggered Wikipedia's anti-abuse mechanism, blocking all non-registered UK users from editing articles.[307] Electronic Frontiers Australia vice-chairman Colin Jacobs commented that "[the] incident in Britain, in which virtually the entire country was unable to edit Wikipedia because the [IWF] had blacklisted a single image on the site, illustrated the pitfalls of mandatory ISP filtering."[308] Facing a storm

---

unprecedented step of banning users in Britain from accessing a Wikipedia web page, which contains an album cover featuring an image of a young nude girl."); Wikipedia Child Image Censored, BBC (Dec. 8, 2008), http://news.bbc.co.uk/2/hi/7770456.stm ("Some volunteers who run Wikipedia said it was not for the [IWF] to censor one of the web's most popular sites.").

303. *See* Claudine Beaumont & Nicole Martin, *Wikipedia Ban Lifted by Internet Watch Foundation*, THE TELEGRAPH, (Dec. 10, 2008), http://www.telegraph.co.uk/technology/news/3700396/Wikipedia-ban-lifted-by-Internet-Watch-Foundation.html (reporting on IWF's decision to lift the Wikipedia ban resulting from the Scorpions' Virgin Killer album cover); Bobbie Johnson, *Wikipedia falls foul of British censors*, THE GUARDIAN, (Dec. 7, 2008), http://www.theguardian.com/technology/2008/dec/08/wikipedia-censorship (reporting on the result of IWF's blacklist of Wikipedia page).

304. Wikipedia Child Image Censored, BBC (Dec. 8, 2008), http://news.bbc.co.uk/2/hi/7770456.stm (detailing the IWF's response); *see supra* notes 303 (reporting on the IWF's response to the Wikipedia page).

305. *See Censorship of WP in the UK Dec 2008 Q&A*, WIKIMEDIA FOUND., http://wikimediafoundation.org/wiki/Censorship_of_WP_in_the_UK_Dec_2008QA (last visited Dec. 30, 2014) (explaining why UK users were unable to edit the Wikipedia page); Jeremy Kirk, *Wikipedia Article Censored in UK for the First Time*, PCWORLD (Dec. 8, 2008), http://www.pcworld.com/article/155112/wikipedia_censored.html (describing the unintended effects of blacklisting a Wikipedia article) .

306. Since at least ninety-five percent of UK Internet users subscribe to ISPs that utilize the IWF's blacklist, a significant number of UK subscribers were unable to edit the Wikipedia page. Jeremy Kirk, *Wikipedia Article Censored in UK for the First Time*, PCWORLD (Dec. 8, 2008), http://www.pcworld.com/article/155112/wikipedia_censored.html; *see also supra* notes 303-05 (explaining the reason UK users were unable to edit the Wikipedia page).

307. *See supra* notes 303-06 (describing inadvertent mass blocking resulting from IWF's blacklist and Wikipedia's internal mechanisms).

308. *See* Asher Moses, *Labor Plan to Censor Internet in Shreds*, SYDNEY MORNING HERALD (Dec. 9, 2008), http://www.smh.com.au/news/home/technology/labor-plan-to-censor-Internet-in-shreds/2008/12/09/1228584820006.html?page=fullpage#contentSwap1 (reporting concerns over Australia's proposal to adopt an Internet censorship system similar to the IWF);

of controversy, the IWF rescinded the block on December 9, 2008 after conducting its own independent, nontransparent appeal process.[309]

In efforts to provide accountability and reassure stakeholders, the IWF regularly invites independent auditors to inspect the organization's processes.[310] In November 2013, Lord Ken Macdonald of River Glaven, Director of Public Prosecution, conducted a human rights audit of the IWF.[311] In his report dated January 27, 2014, Lord Macdonald recommended several improvements, such as increasing the transparency in the inspection and appeal process.[312] The IWF adopted seven of the recommendations, including appointing a human rights expert on the Board and appointing a senior legal figure as the Chief Inspector of the appeals process.[313] While these improvements would likely improve the IWF processes, the blocking resulting from ISPs utilizing the IWF's URL list continues to be opaque.

Further, the trend of graduated response laws has prompted international attention from human rights scholars.[314] Special Rapporteur La Rue challenged the legitimacy of graduated response laws, declaring that "[c]utting off subscribers from Internet access, on

---

see also Colin Jacobs, *The Future of Internet Censorship*, ELECTRONIC FRONTIERS AUSTRALIA, (Sept. 21, 2010) (referencing the IWF and Wikipedia incident)..

309. *See* Jacqui Cheng, *IWF Backs off of Scorpions Wikipedia Block After Criticism*, ARS TECHNICA (Dec. 9, 2008), http://arstechnica.com/tech-policy/2008/12/iwf-backs-off-of-scorpions-wikipedia-block-after-criticism/ (reporting that "the fact that the image is some 32 years old and posted pretty much everywhere on the Internet. . . has prompted the IWF to remove it from its list of illegal content."); Richard Korman, *British Watchdogs Back Down Over Wikipedia Image of Nude Girl*, ZDNET (Dec. 9, 2008), http://www.zdnet.com/blog/government/british-watchdog-backs-down-over-wikipedia-image-of-nude-girl/4214 (reporting the IWF's lift of the ban).

310. *See Independent Inspection*, INTERNET WATCH FOUND., https://www.iwf.org.uk/accountability/independent-inspection (last visited Dec. 30, 2014) (providing the public with the auditor's reports); *see, e.g.*, 2013 AUDIT OF THE INTERNET WATCH FOUNDATION (Jul. 19, 2013), https://www.iwf.org.uk/assets/media/accountability/IWF%20Hotline%20Audit%202013.pdf (reporting a satisfactory inspection of the IWF's processes).

311. *See Human Rights Audit*, INTERNET WATCH FOUND., https://www.iwf.org.uk/accountability/human-rights-audit (last visited Dec. 30, 2014) (providing the public with the auditor's reports) (reporting the adoption of several of Lord Macdonald's recommendations).

312. *See* Macdonald, *supra* note 299, at 25 ("It is critical . . . that IWF's inspection process should be transparent and properly designed).

313. *Human Rights Audit*, INTERNET WATCH FOUND., https://www.iwf.org.uk/accountability/human-rights-audit (last visited Dec. 30, 2014) (reporting the adoption of several of Lord Macdonald's recommendations).

314. *See, e.g.*, May 2011 La Rue Report, *supra* note 53, at 14 (expressing his deep concerns over discussions regarding a centralized on/off control over Internet traffic).

the grounds of violating intellectual property rights law, is completely disproportionate and subsequently a violation of Article 19, Paragraph 3, of the [ICCPR]."[315] The Special Rapporteur urges States Parties to repeal or amend existing intellectual copyright laws, which permit users to be disconnected from Internet access, and to refrain from adopting such laws.[316]

Prime Minister Cameron's proposal of default filtering of legal content raises several human rights issues.[317] For example, Special Rapporteur La Rue noted that "while the protection of children from inappropriate content may constitute a legitimate aim, the availability of software filters that parents . . . can use to control access to certain content renders action by the Government such as blocking less necessary and difficult to justify."[318] Similarly, Jim Killock, executive director of the Open Rights Group, explains that default filters may not be necessary.[319] The underlying issue can be addressed by increasing funds for the policing of the criminals responsible for the production and distribution of images of child abuse.[320] While the effects of the United Kingdom's default filter proposal and its graduated response law can be analyzed under the traditional Article 19 analysis, the UK ISP's cooperation with a nongovernment organization muddles the analysis. The narrowed scope of Article

315. *Id*. at 21.

316. *See id*.

317. *See* May 2011 La Rue Report, *supra* note 53, at 10 (stating that States' use of blocking or filtering technologies is often in violation of their obligation to guarantee the right to freedom of expression); *Joint Declaration*, *supra* note 279, at 3 ("Content filtering systems which are imposed by a government or commercial service provider and which are not end-user controlled are a form of prior censorship and are not justifiable as a restriction on freedom of expression.").

318. May 2011 La Rue Report, *supra* note 53, at 9 (recognizing that advances in technology are weakening governments' justifications for censorship based on protecting children from inappropriate content).

319. *See* Jim Killock, *David Cameron is Issuing Bad Advice to Parents*, OPEN RIGHTS GROUP BLOG (Jul. 22, 2013) https://www.openrightsgroup.org/blog/2013/porn-blocks-edging-away-from-active-choice (arguing for that the proposed filters are not feasible); Jim Killock, *Help us to Re-start the Debate About Internet Filters*, OPEN RIGHTS GROUP BLOG (Apr. 15, 2014), https://www.openrightsgroup.org/blog/2014/help-us-to-restart-the-debate-about-Internet-filters (launching campaign to raise awareness of the Internet filtering issue).

320. *See* Killock, *supra* note 320 (arguing that mandatory filters are not required to protect children); *see also* Olly Lenard, *Why David Cameron's Internet Censorship Is a Terrifying and Terrible Idea*, HUFFINGTON POST UK BLOG (Jul. 29, 2013, 10: 52 PM), http://www.huffingtonpost.co.uk/olly-lennard/why-david-camerons-intern_b_3653566.html (arguing that that Prime Minster Cameron's proposed filtering measures are ineffective, ill-informed and bound to fail).

19(3) to laws or actions of the government possibly limits the actions and decisions of non-government actors, such as ISPs and the IWF, from the purview of the ICCPR.

C. *Article 19 Analysis of China: Examining the "Impregnable Fortress"*

China's policy of Internet censorship has drawn international attention and criticism.[321] China's content regulation scheme comprises a morass of statutes, regulations, and decrees from numerous government entities.[322] Although China is a signatory to the ICCPR, the Chinese government has not ratified the treaty.[323] Establishing the potential violations of Article 19 will illuminate the extent of the PRC's human rights violations, and subsequently establish grounds to remedy them. While Article 19(3) permits restrictions for the protection of national security, public order, health and morals, these restrictions must comply with the three-part cumulative test expressed in Article 19(3).[324] A closer examination reveals that the PRC's regulation of the Internet suffers from vagueness, disproportional sanctions, and lack of transparency.[325]

Imprecise language creates difficulty in determining which speech is permitted and which are prohibited.[326] For instance, the *Regulation on Publication Administration* provides that "no

---

321. *See e.g.*, *supra* notes 216-36 (discussing international criticism of PRC's control over their internal Internet activity).

322. *See supra* Part I.D.1-2 (discussing the methods and effects of China's manipulation of the Internet).

323. Signing a treaty is a step towards becoming party to a treaty. *See Understanding International Law Fact Sheet #5*, UNITED NATIONS, https://treaties.un.org/doc/source/events/2008/Press_kit/fact_sheet_5_english.pdf ("A State can express its consent to be bound in several ways . . . the most common ways are: definitive signature, ratification, acceptance, approval, and accession.").

Simply signing a treaty, however, does not usually make a State a party. *Id.* Signing treaties does, however, create an obligation, in the period between signature and ratification to refrain in good faith from acts that would defeat the object and purpose of the treaty. *Id.*

324. *See* ICCPR, *supra* note 5, art. 19(3).

325. *See infra* notes 327-58 (describing the vagueness of various regulations, disproportional punishment of Internet bloggers and critics, and lack of transparency of the Golden Shield Project).

326. *See* Mindy Kristin Longanecker, *No Room for Dissent: China's Laws Against Disturbing Social Order Undermine Its Commitments to Free Speech and Hamper the Rule of Law*, 18 PAC. RIM L. & POL'Y J. 373, 398 (2009) (discussing how laws against disturbing social order are vague and leave citizens and officials without proper guidance as to the laws' scope); Shao, *Internet Speech*, *supra* note 196, at 56-57 (discussing the lack of certainty caused by vague laws).

publication" may contain content "harming the honor or the interest of the nation" and "disturbing social order, disrupting social stability."[327] What constitutes honor, national interest, social order, and social stability are not defined.[328] Furthermore, the aforementioned prohibition is also present in numerous statutes such as the *Criminal Law* and *Decision on Safeguarding Internet Security*.[329]

In addition, the involvement of various regulatory and licensing agencies constitutes a form of prior restraint.[330] The GAPP requires all proposed publications on "important topics" to be filed with their agency.[331] The PRC further requires individuals or organizations to obtain permits in order to lawfully engage in media business.[332] The *Regulation on Internet Information Service* requires all commercial

---

327. Chuban Guanli Tiaoli (2011 Xiuding) (出版管理条例(2011修订)) [Regulation on the Administration of Publication (2011 Revision)] (promulgated by State Council, Mar. 19, 2011, effective Jul. 18, 2013) (Lawinfochina) (China) (failing to delineate the scope of what constitutes "disturb[ing] the public order or destroy[ing] the public stability.").

328. *See id.*; Longanecker, *supra* note 327, at 399 (noting the lack of definitions of key terms in PRC regulations).

329. *See* Zhonghua Renmin Gongheguo Xingfa (97 Xiuding) (中华人民共和国刑法(97修订)) [Criminal Law of the People's Republic of China (97 Revision)] (promulgated by National People's Congress, Mar. 14, 1997, effective Oct. 1 1997) (Lawinfochina) (China) (failing to define the terms); Quanguo Rwn Da Chang Weihuì Guanyu Weihu Hulianwang Anquan De Juedìng (全国人大常委会关于维护互联网安全的决定) [Decision of the Standing Committee of the National People's Congress on Preserving Computer Network Security] (promulgated by Standing Committee of the National People's Congress, Dec. 28, 2000, effective Dec. 28, 2000) (Lawinfochina) (China) (failing to define the terms).

330. *See* Shao, *Regulating the Internet*, *supra* note 199, at 54-56 (explaining that China's licensing schemes amount to prior restraint); *Prior Restraints*, CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA, http://www.cecc.gov/prior-restraints (last visited Dec. 30, 2014) (listing the various forms of prior restraint in China).

331. These topics include: literature of the Party or the nation, former or current leaders of the Party or the nation, Party secrets or state secrets, nationality problems or religious problems, the Cultural Revolution, the former Soviet Union, and Eastern European bloc. *See* [Guanyu Yinfa Tushu Qikan Yinxiang Zhipin Dianzi Chubanwu Zhongda Xuan Tili Beian Banfa De Tongzhi(关于印发(图书、期刊、音像制品、电子出版物重大选题备案办法)的通知) [Measures on the Recording of Important Topics of Books, Periodicals, Audio/Visual Productions and Electronic Publications]promulgated by the General Office of the General Administration of Press, October 10, 1997, effective October 10, 1997), http://www.cecc.gov/resources/legal-provisions/circular-regarding-the-printing-and-promulgation-of-the-measures-on-the#body-chinese (China); *see also* Shao, *Regulating the Internet*, *supra* note 199, at 55 (describing the GAPP's licensing procedures).

332. *See, e.g.*, Hulianwang Xinxi Fuwu Guanli Banfa (互联网信息服务管理办法) [Regulation on Internet Information Service] (promulgated by the State Council, Sept. 25, 2000, effective Jan. 8, 2011) (Lawinfochina) (China) (requiring individuals to obtain a license before engaging in the media business).

and non-commercial Internet information services to file with their local telecommunications regulatory authority.[333] Similarly, the *Administration of the Publication of Audio-Visual Programs* stipulates that no one may operate an Internet broadcast business for news-related audio/visual programs without permission from the State Council Information Office.[334] Consequently, the Chinese government controls the amount, structure, distribution, and coordination of publishing and broadcasting within the country.[335]

Vague language and overbreadth are legal comorbidities.[336] Numerous regulations become over-inclusive and prohibit an expansive set of activities by using imprecise language.[337] For instance, the *Regulations on the Administration of Business Sites of Internet Access Services* proscribes that no unit or individual may utilize the Internet to produce, copy, look up, or transmit information "damaging the interest of the state."[338] This statute ostensibly prohibits the use of the Internet to criticize the Chinese

---

333. *See id*.

334. Hulianwang Deng Xinxi Wangluo Chuanbo Shi Jiemu Guanli Banfa (互联网等信息网络传播视听节目管理办法) [Measures for the Administration of the Publication of Audio-Visual Programs through the Internet] (promulgated by State Broadcasting, Film and TV Administration, July 6 2004, effective Oct. 11, 2004) (Lawinfochina) (China) ("The License for Publication of Audio-Visual Programs through Information Network shall be obtained for undertaking the business of publication of audio-visual programs through information network.").

335. *See* Shao, *Regulating the Internet, supra* note 200, at 55 (describing the PRC's control over publishing and broadcasting). In addition to licensing and reporting schemes, the Chinese government also proactively takes down search engines, online chat rooms and blog service providers. *See* Raymond Li and Kristine Kwok, *Popular Forum Rushes to Go Offline After Closure Order*, SOUTH CHINA MORNING POST (Jul. 26, 2006), http://www.scmp.com/article/558028/popular-forum-rushes-go-offline-after-closure-order (reporting that a popular online forum has been ordered to shut down after mainland authorities began tightening their grip on the Internet).

336. *See* Richard H. Fallon, Jr., *Making Sense of Overbreadth*, 100 YALE L.J. 853, 857 (1991) (arguing that vagueness is best analyzed as a subcategory of overbreadth and that overbreadth principles should govern vagueness issues); Shao, *Regulating the Internet*, *supra* note 202, at 57 (noting that vagueness and overbreadth are often overlapping).

337. *See* Longanecker, *supra* note 327, at 399 (noting that when the laws present ambiguous terms without any guidance for government officials or citizens, Chinese police and courts interpret these terms inconsistently); Shao, *Regulating the Internet*, *supra* note 200, at 57 (explaining that vague laws risk selective enforcement and may proscribe a broad range of activities).

338. Hulianwang Shangwang Fuwu Yingye Changsuo Guanli Tiaoli (互联网上网服务营业场所管理条例) [Regulations on the Administration of Business Sites of Internet Access Services] (promulgated by State Council, Sept. 29, 2002, effective Nov. 15, 2002) (Lawinfochina) (China), art. 14 (prohibiting the use of the Internet to harm the social ethics or the excellent cultural traditions of the nationalities).

government.[339] While the Supreme People's Court and Supreme People's Procuratorate have issued various interpretation guidelines, this does not solve the underlying problem of vague regulations and instead only amounts to a short fix to a deeper problem.[340]

The government's control over the Internet is further reinforced by the installation of the Great Firewall of China.[341] The firewall raises numerous potential Article 19 violations, including preventing citizens from receiving and seeking information.[342] For instance, a search for "Human Rights Watch" on a Chinese ISP will return an error page.[343] Unlike other countries, such as Saudi Arabia, where blocked content is redirected to a page explaining the reason why the content is blocked, access to restricted content in China only informs the user that "connection was reset."[344] Therefore, intentional censorship is difficult to distinguish from a technical error.[345]

The PRC recently increased surveillance of Internet activity, specifically microblogs, which are more concise and thematic versions of traditional blogs.[346] The threat of harsh sanctions can exert

---

339. *See id*.

340. *See* 2010 Judicial Interpretation, *supra* note 210 (attempting to give guidance to government officials regarding the scope of pornography laws); Longanecker, *supra* note 327, at 399 (arguing that in order restore legitimacy of certain laws, China needs to address the vague terminology).

341. *See* Lyombe Eko, Anup Kumar & Qingjiang Yao, *Google This: The Great Firewall of China, the It Wheel of India, Google Inc., and Internet Regulation*, 15 J. INTERNET L. 3, 5 (2011) ("The Great Firewall Wall of China is a massive, sophisticated, national censorship system that uses a number of techniques . . . to automatically control and restrict the stream of Internet communication entering or leaving China . . . ."); Shao, *Regulating the Internet*, *supra* note 200, at 43 (explaining China's use of a variety of technical measures to filter content).

342. *See* ICCPR, *supra* note 5, art. 19(1)(2).

343. *See* Bambauer, *Cybersieves*, *supra* note 21, at 391 (explaining China's lack of openness regarding their use of filters); *"Race to the Bottom" Corporate Complicity in Chinese Internet Censorship*, HUMAN RIGHTS WATCH, Aug. 2006, Vol. 8 No. 8, 10-11 [hereinafter *Race to the Bottom*] (describing the extent of the PRC's control over the Internet at the router-level).

344. *Race to the Bottom*, *supra* note 343, at 11 (discussing that governments differ in their attempts to inform the Internet user about blocked content); *see* Bambauer, *Cybersieves*, *supra* note 21, at 391-92 (juxtaposing the openness of Saudi Arabia's use of filters with the lack of openness of Great Firewall of China); Alfred Hermida, *Saudis Block Two Thousand Websites*, BBC (Jul. 31, 2002) http://news.bbc.co.uk/2/hi/technology/2153312.stm (reporting that the Saudis are also open about their censorship of the web).

345. *See* Bambauer, *Cybersieves*, *supra* note 21, at 391 (noting that intentional censorship is difficult to distinguish from technical errors); *Race to the Bottom*, *supra* note 344, at 10 (explaining the China's filters causes an error message to appear in the users' browser when they searched for blocked content).

346. *See* Chen, *supra* note 20, at 250 (discussing the extent of Internet monitoring in China); *China Employs Two Million Microblog Monitors State Media Say*, BBC (Oct. 4,

a significant chilling effect on the right to freedom of expression.[347] China currently leads the word in number of arrested Internet users, coined "netizens."[348] Among the current prisoners are a Nobel Peace Prize winner and number of human rights activists.[349]

On January 31, 2005, Changsha's prosecutorial office, the People's Procuratorate of Changsha, Hunan, filed charges against Shi Tao for illegally providing state secrets outside the country.[350] Shi Tao was the head of the Editorial Department of Hunan's Contemporary Business News and used his personal Yahoo! e-mail account to send allegedly top-secret documents to the Asia Democracy Foundation, a website located in New York that advocates for democracy in China.[351] Shi Tao was sentenced to ten years imprisonment with two years of subsequent deprivation of political rights.[352] This case garnered worldwide attention because an American corporation, Yahoo!, aided in Shi Tao's arrest by willingly disclosing details of Shi Tao's email to the Chinese government.[353]

2013), http://www.bbc.com/news/world-asia-china-24396957 (reporting the expansion of China's Internet monitoring task force).

347. *See* John D. Zelezny, COMMUNICATION LAW: LIBERTIES, RESTRAINT AND MODERN MEDIA 50-51 (6th ed. 2011) (explaining that subsequent punishment may chill expression as much as prior restraints); Shao, *Regulating the Internet*, *supra* note 200, at 56 (noting that when punishment is overly harsh, the prospects of subsequent sanctions may serve to chill expression as much as prior orders not to publish).

348. *See Internet Enemies 2012 – China*, REPS. WITHOUT BORDERS (Mar. 12, 2012) https://en.rsf.org/china-china-12-03-2012,42077.html (last visited Dec. 30, 2014) (reporting the waves of blogger and "netizen" arrests); *see also China Arrests Blogger for Twitter Joke*, THE GUARDIAN, (Nov. 21, 2012), http://www.theguardian.com/world/2012/nov/21/china-arrest-blogger-twitter-joke (reporting an arrest of a Chinese Twitter user for making jokes about the Chinese Congress).

349. Liu Xiaobo, a professor, Nobel Peace Prize laureate, and human rights activist, is currently incarcerated as a political prisoner in China. *See* Mark Mcdonald, *An Inside Look at China's Most Famous Political Prisoner*, N.Y. TIMES BLOG (Jul. 23, 2012) http://rendezvous.blogs.nytimes.com/2012/07/23/an-inside-look-at-chinas-most-famous-political-prisoner/?_php=true&_type=blogs&_r=0 (reporting about Liu Xiaobo's sentence for seeking democractic reforms); *Internet Enemies 2011 – China*, REPS. WITHOUT BORDERS (March 11, 2011) *available at* http://www.refworld.org/docid/4d822690c.html (Reporting on human rights activist, Hu Jia's, sentence for inciting subversion of state power).

350. *See* Shi Tao (Hunan Province, Changsha Intermediate People's Ct. 2003) [April 27, 2005], *available at* http://www.globalvoicesonline.org/wp-content/ShiTao_verdict.pdf (finding that defendant Shi Tao intentionally and illegally provided information that he knew to be top-secret level state secrets to an entity outside of the country)*;* Shao, *Internet Speech*, *supra* note 196, at 79-82 (summarizing the *Shi Tao* case).

351. *See supra* note 350 (describing the *Shi Tao* case).

352. *Id*.

353. *See* Shyu, *supra* note 224, at 228 ("Because he sent the email from his Yahoo! account, China requested, and Yahoo! Hong Kong delivered, information on Shi Tao's

Moreover, the reported treatment of political prisoners may also cause a chilling effect on speech.[354] For instance, cyber-dissident Zhang Jianhong, better known under his pen name Li Hong, died of complications from a disease that was untreated during three years in prison for writing articles critical of the Chinese government.[355] The incarceration of bloggers and cyber-dissidents clearly runs afoul with proportionality principles of Article 19.[356]

The analysis in Part II demonstrates that Article 19 is not adequate to tackle the modern challenges presented by the government. US and UK intellectual property laws present collateral effects on expression that are not easily analyzed under Article 19. Moreover, it is also unclear about Article 19's scope vis-à-vis the active role of nongovernment organization in the Internet censorship. However, an Article 19 analysis is clearest when dealing with a totalitarian government, such as the PRC.

III. *ARTICLE 19 NEEDS HELP TO STAY RELEVANT IN THE INTERNET AGE*

While the HRC's interpretations helps to construe the scope of Article 19, the margin of discretion that is potentially accorded to nations exemplifies the difficulty of analyzing countries with

---

location."); *Undermining Freedom of Expression in China*, AMNESTY INT'L, (July 2006), http://www.ethicsworld.org/corporatesocialresponsibility/PDF%20links/Amnesty.pdf (reporting on the treatment of Shi Tao and his family by the government).

354. *See* Mayton, *supra* note 11, at 253-54 (explaining how subsequent punishment may chill freedom of expression); Zelezny, *supra* note 348, at 50-51 (describing the effects of subsequent punishment on speech).

355. *See Zhang Jianhong (Pen Name: Li Hong)*, PEN AMERICA, http://www.pen.org/defending-writers/test-first-name-test-middle-name-test-last-name/zhang-jianhong-pen-name-li-hong (last visited Dec. 30, 2014) ("Zhang Jianhong's condition worsened considerably due to a prolonged lack of medical care, and repeated applications for medical parole were denied despite his declining health."); Richard Finney, *Cyber-Dissident Dies on Parole*, RADIO FREE ASIA (Jan. 5, 2011), http://www.rfa.org/english/news/china/dissident-01052011131836.html ("An outspoken Chinese cyber-dissident has died after suffering from an untreated medical condition in jail, according to friends.").

356. *See* UN General Comment 34, *supra* note 51 (requiring State to invoke a legitimate ground in order to restrict the right to freedom of expression); May 2011 La Rue Report, *supra* note 52, at 11 (affirming Human Rights Council declaration that restrictions should never be applied, inter alia, to discussion of Government policies and political debate, and reporting on human right).

divergent laws and norms.[357] This difficulty created by transnational norms is further exacerbated when the Internet is involved.

Moreover, although Article 19 was drafted with the foresight to accommodate future technology, the Internet has developed into a phenomenon that cannot be adequately governed by traditional media laws.[358] For instance, the absolute language in Article 19, Paragraph 2, can lead to possible conflicts for countries that are also parties to the WIPO Treaty and the Berne Convention.[359] While these international copyright agreements do not explicitly require implementing a notice-and-action regime, numerous governments have adopted this type of intermediary liability system.[360] This growing trend of intermediary liability has caused the Special Rapporteurs and the HRC to recognize that current notice-and-action systems are likely incompatible with Article 19.[361]

In order to adapt international human rights law to the new challenges presented by the Internet, Article 19 should be supplemented by parts of Professor Bambauer's process-based framework delineated in *Cybersieves*. This metric utilizes normative criterion for analyzing a censorship system: openness, narrowness, transparency, and accountability.[362] Although Article 19 already incorporates similar principles, the enumerated principles only establish baseline rights and a positive duty for State members to promote access to the Internet.[363]

---

357. *See, e.g.*, Human Rights Comm., Hertzberg Commc'n*, supra* note 238 ("There is no universally applicable common standard. Consequently, in this respect, a certain margin of discretion must be accorded to the responsible national authorities."); Legg, *supra* note 242, at 141 ("One of the most powerful criticisms of the margin of appreciation doctrine is that it panders to relativist notions of human rights law, which ought to be universal.").

358. *See* May 2011 La Rue Report, *supra* note 53, at 8 (emphasizing that due to the unique characteristics of the Internet, regulations which may be deemed legitimate for traditional media are often not so with regard to the Internet).

359. *See* ICCPR, *supra* note 5, art. 19(2).

360. *See supra* notes 113-19 (discussing the DMCA); *supra* notes 176-81 (discussing the E-Commerce Directive).

361. *See generally Joint Declaration*, *supra* note 279, § 2(a-b) (declaring that no one "should be liable for content generated by others, which is disseminated using those services, as long as they do not specifically intervene in that content or refuse to obey a court order to remove that content, where they have the capacity to do so"); May 2011 La Rue Report, *supra* note 53, at 11 (noting that intermediary liability systems are subject to abuse).

362. *See* Bambauer, *Cybersieves*, *supra* note 21, at 390-411 (establishing the framework).

363. ICCPR, *supra* note 5, art. 19.

As demonstrated by the limited HRC cases, the protection of these rights is muddled by divergent norms and values.[364] Unlike the text of Article 19, an analysis under the framework does not rely solely on asking why a country regulates Internet content, for which there are possibly infinite reasons, but instead the framework asks *how* the country regulates the Internet.[365] Moreover, because the metric encompasses culturally-neutral normative values, incorporating these aims will improve the analysis of different countries' Internet governance. The metric essentially converts abstract principles into concrete, measurable evaluations.

The first criterion is openness. The framework looks to whether the country admits to the filtering and clearly describes the justifications for such filters.[366] In other words, openness assesses whether a state discloses why it censors. Censorship that is disclosed and explained is likely to be seen as more legitimate than covert censorship.[367] Openness is readily achievable with the current state of filters.[368] For instance, Saudi Arabia's Internet filters redirect blocked content to a webpage that informs the Internet user about the country's censorship policy.[369]

The second criterion is transparency. While transparency and openness are concomitant, transparency relates to the opacity of the specific content that is filtered and the criteria that the government uses to delineate prohibited content from permissible content.[370] Transparent filtering allows end-users to assess how the blacklist

---

364. *See supra* notes 237-41 (discussing the HRC's lack of progress in respects to freedom of expression cases).

365. *See* Bambauer, *Cybersieves*, *supra* note 21, at 390 (describing that the goal of the framework is to evaluate how well a country describes what it censors).

366. *See* Bambauer, *Cybersieves*, *supra* note 21, at 390 (explaining the openness criterion); Bambauer, *Orwell's Armchair*, *supra* note 10, at 900-06 (analyzing specific soft censorship models under the Framework).

367. *See* Bambauer, *Cybersieves*, *supra* note 21, at 390-92 (discussing the standard of openness); *see also* Bambauer, *Orwell's Armchair*, *supra* note 10, at 900-01 (discussing the general lack of openness of soft censorship resulting from government persuasion).

368. *See* Bambauer, *Cybersieves*, *supra* note 21, at 392 (discussing that current filtering technology can display a block page when a user is prevented from accessing banned material); Saudi Internet Rules, *supra* note 246 (proscribing specific Internet activities and content).

369. *See Race to the Bottom*, *supra* note 344, at 11 (noting that attempting to access blocked webpages in Saudi Arabia will redirect users to an information page); Saudi Internet Rules, *supra* note 246 (notifying users of the prohibited content).

370. *See* Bambauer, *Cybersieves*, *supra* note 21, at 393 (explaining the transparency criterion); Bambauer, *Orwell's Armchair*, *supra* note 10, at 902-03 (discussing the lack of transparency in soft censorship methods).

conforms to the government's justifications for information control.[371] Moreover, the transparency criterion can also apply to copyright laws. For instance, a transparent notice-and-action system discloses its criteria and publicly records its notices. Despite Article 19's similar requirements of openness and transparency, the framework provides for a more detailed, concrete guideline for analyzing a system's openness and transparency.

The third criterion, narrowness, analyzes the accuracy of what a country actually blocks to the government's description of its censorship.[372] Narrowness examines both over-inclusiveness and under-inclusiveness censorship.[373] Over-inclusive censorship can be deliberate or inadvertent.[374] For instance, inadvertent filtering can result from classification errors.[375] The Golden Shield Project, on the other hand, exemplifies deliberate over-inclusive censorship because it utilizes sophisticated content-filtering technology that purportedly blocks any websites containing selected keywords.[376]

Under-inclusive censorship occurs when users can routinely reach banned content.[377] The CleanFeed system is an example of under-inclusive filters because the CleanFeed system utilizes the IWF's URL list, which requires regular updates from citizen reports.[378] Consequently, the filters are a step behind the creators of illegal content. Some argue that under-inclusiveness harms the

371. *See* Bambauer, *Cybersieves*, *supra* note 21, at 393 (discussing the transparency criterion); Bambauer, *Orwell's Armchair*, *supra* note 10, at 902-03 (discussing the lack of transparency in soft censorship methods).

372. *See* Bambauer, *Cybersieves*, *supra* note 21, at 396 (detailing the narrowness criterion); Bambauer, *Orwell's Armchair*, *supra* note 10, at 903-06 (arguing that soft censorship methods also typically fare poorly on the narrowness criterion).

373. *See* Bambauer, *Cybersieves*, *supra* note 21, at 396-401 (discussing over and under-inclusive censorship); Bambauer, *Orwell's Armchair*, *supra* note 10, at 903-06 (discussing how soft-censorship methods can be either over and under-inclusive).

374. *See* Bambauer, *Cybersieves*, *supra* note 21, at 397 (giving examples of over-inclusive censorship); Bambauer, *Orwell's Armchair*, *supra* note 10, at 903-06 (discussing the effects of inadvertent over-inclusive soft-censorship methods).

375. *See* Bambauer, *Cybersieves*, *supra* note 21, at 397 (discussing examples of inadvertent over-inclusive filtering).

376. *See supra* notes 216-27 (discussing the rationale behind implementing the Great Firewall of China).

377. *See* Bambauer, *Cybersieves*, *supra* note 21, at 396-99 (giving examples of under-inclusive censorship); Bambauer, *Orwell's Armchair*, *supra* note 10, at 903-06 (arguing that various forms of soft censorship models can also be under-inclusive).

378. *See supra* notes 150-64 (explaining the IWF process and the CleanFeed mechanism).

legitimacy of the Internet censorship regime.[379] For instance, during the IWF-Wikipedia incident, one of the leading criticisms of the IWF was that the blocked album cover could be accessed elsewhere on the Internet.[380] Because of the constant advancement of technology and the continual growth of the Internet's seemingly endless expanse, however, moderate levels of under-inclusiveness is to be expected, and should be tolerated.

The inclusion of the narrowness metric to the current Article 19 analysis will also allow for a clearer understanding of the chilling effects caused by copyright laws. For instance, by collecting and examining empirical data of a notice-and-action system, auditors will be able to determine the accuracy of a system's process and extrapolate inferences about its effect on Internet speech.[381]

The final criterion is accountability, which takes into account the degree that citizens influence censorship policy.[382] Accountability is further divided into citizen participation, specification of authority, opportunity to challenge, and counter-majoritarian constraints.[383] This criterion creates problems when applied to non-democratic countries. The sub-prongs are intrinsically tied to democratic ideals and, as a result, a positive analysis of the final criterion relies heavily on whether the country is democratic.[384] Professor Bambauer offers Saudi Arabia, a monarchy, as a counterexample by referencing the

379. *See, e.g.*, Bambauer, *Cybersieves*, *supra* note 21, at 398-99 ("filtering that fails to block forbidden material--especially badly flawed or nominal blocking--undercuts the justification for restricting access."); Bambauer, *Orwell's Armchair*, *supra* note 10, at 904-05 (discussing the failure of New York Governor Cuomo's persuasion-based soft-censorship).

380. *See supra* notes 301-09 (describing the IWF-Wikipedia incident).

381. *See, e.g.*, Urban & Quilter, *supra* note 116, at 624 (describing efforts from different organizations on gathering information on notice-and-takedown requests and examining the data); CHILLING EFFECTS PROJECT, *supra* note 289 (studying cease and desist letters concerning online content).

382. *See* Bambauer, *Cybersieves*, *supra* note 21, at 400 (discussing the accountability criterion); Bambauer, *Orwell's Armchair*, *supra* note 10, at 927 (discussing that while SOPA and PIPA fare poorly on the other criterion, the acts of Congress score well on the accountability criterion).

383. *See* Bambauer, *Cybersieves*, *supra* note 21, at 400-01 (discussing the accountability criterion).

384. Experts have regarded accountability and citizen participation as key elements of a democratic society. *See, e.g.*, August 2011 La Rue Report, *supra* note 52 (noting that civic participation is conducive to a democratic society); Bambauer, *Cybersieves*, *supra* note 21, at 404-10 (discussing how several select nondemocratic countries fail at several aspects of accountability).

country's citizen participation in Internet censorship. [385] However, because of the limited political participation in the country, Saudi Arabia fares poorly on the remaining sub-prongs, such as opportunity to challenge and counter-majoritarian restraints. While accountability is important, imposing democratic virtues on non-democratic governments is counter-productive. Non-democratic State parties will likely fare poorly in the accountability analysis, and requiring those governments to adhere to democratic ideals may be seen as attempts at undermining the nation's sovereignty. This Note is not arguing that non-democratic governments are intrinsically incompatible with the accountability criterion; rather that the international community should not impose the aforementioned democratic principles on countries that are not ready to transition into a democracy. For these reasons, accountability should be the least weighed factor.

Furthermore, Professor Bambauer is correct to recognize that a framework is only as useful as its implementation.[386] In order to determine the weight given to each criterion, he argues that competition between public and private stakeholders is most efficient method to develop the most efficient version of the framework.[387] Professor Bambauer further argues that while there are other means of implementation, such as collaboration between stakeholders, and a top-down process, they present various challenges.[388] For instance, collaboration between parties may lead to gridlock or conflicts of interest, while a top-down implementation may unintentionally promote the stakeholder's concept on free expression.[389]

Despite Professor Bambauer's reservation on designating the implementation process to a single entity, this Note argues that top-down implementation can be more expedient, efficient, and neutral than the other methods with the correct stakeholder. Since the HRC is

---

385. *See* Bambauer, *Cybersieves*, *supra* note 21, at 404 (referencing Saudi Arabia as a country that permits only limited political participation but invites citizen participation in respect to Internet censorship).

386. *Id.* at 410 (recognizing the importance of effective implementation for the possibility of the framework's success).

387. *Id.* at 414 (arguing that with competition, proposed metrics should get better and fewer over time).

388. As the name suggests, the collaborative models involve various stakeholders collaborating on the implementation of the framework. *Id.* at 416-17 (describing the collaborative model). The top-down model involves a powerful stakeholder to press for the framework's adoption. *Id.* at 416-17 (discussing the top-down model).

389. *Id.* at 416-17 (explaining the various defects of each alternative models of implementing the metric).

an independent organization comprised of individuals from various countries and recognized for their human rights achievements, it is a capable organization to develop and adopt the framework.[390] Moreover, the HRC is already tasked with the analytic review of reports and releases observations based on its findings.[391]

CONCLUSION

Each country's method of Internet censorship is to an extent different and idiosyncratic.[392] The United States relies heavily on removing content through private action.[393] The United Kingdom, on the other hand, cooperates with a non-government organization to formulate a blacklist.[394] Lastly, China exercises unilateral domination over its internal Internet activity.[395] The process of supplementing Article 19 with Professor Bambauer's framework arguably will provide the HRC and the global community with more concrete and defined normative aims for their Internet regulatory practice. This is a step towards a global standard for Internet regulation.

390. *See* Carlson, *supra* note 26, at 3 (discussing the roles and capabilities of the HRC); *Monitoring Civil and Political Rights*, *supra* note 36 (describing the role of the HRC); *HRC Fact Sheet 15*, *supra* note 44, at 12-14 (describing the HRC's role).

391. *See* Carlson, *supra* note 26, at 3 (discussing the HRC's compliance mechanisms); *HRC Fact Sheet 15*, *supra* note 44, at 14-30 (describing the HRC's monitoring function).

392. *See supra* Part I.B-D (examining different country's Internet censorship schemes).

393. *See supra* Part I.B (examining the United States' legislative-based model).

394. *See supra* Part I.C (examining the United Kingdom's Internet governance model).

395. *See supra* Part I.D (examining China's extensive regulation of the Internet).