



**From the SelectedWorks of Molly K. Land**

---

January 2013

## Toward an International Law of the Internet

Contact  
Author

Start Your Own  
SelectedWorks

Notify Me  
of New Work

---

Available at: [http://works.bepress.com/molly\\_land/1](http://works.bepress.com/molly_land/1)

# TOWARD AN INTERNATIONAL LAW OF THE INTERNET

MOLLY LAND\*

## TABLE OF CONTENTS

Introduction.....	1
I. A Right to Media.....	2
A. Internet As Right?.....	3
B. The “Media” Clause.....	6
C. After-Arising Technology.....	10
D. The Importance of Means.....	15
II. Applying Article 19(2).....	18
A. Access to Technology.....	19
B. Access to Information.....	25
C. Anonymity Online.....	31
D. Online Borders.....	34
III. Implementing Article 19.....	38
A. Non-State Actors.....	39
B. Human Rights Defaults.....	43
Conclusion.....	50

*“The members of the Commission must take into account the fact that their work concerned the future and not the past; no one could foresee what information media would be employed in a hundred years’ time.”*

– French Delegate to the Sixth Commission on Human Rights, discussing the “media” clause of the article on freedom of expression in the draft human rights covenant on May 2, 1950, Comm’n on Hum. Rts., 6th Sess., ¶ 54, U.N. Doc. E/CN.4/SR.165 (May 2, 1950)

---

\* Associate Professor of Law, New York Law School. My thanks to Derek Bambauer, Troy Elder, Doni Gewirtzmann, James Grimmelman, Dan Hunter, Paul Kahn, Margot Kaminski, Eddan Katz, Rebecca Roiphe, James Silk, and Peter Yu for invaluable feedback. This Article benefitted greatly from the questions and comments of participants in the Yale Human Rights Workshop Series and the Yale Information Society Project’s 15th Annual Reunion Conference. Special thanks to Karen Grushka and all of the librarians at New York Law School for unfailing support in the historical research for this article and to Patrick Boyle for outstanding research assistance.

## ABSTRACT

This Article presents the first and only analysis of Article 19 of the International Covenant on Civil and Political Rights as it applies to new technologies and uses this analysis to develop the foundation for an “international law of the Internet.” Although Article 19 does not guarantee a right to the “Internet” per se, it explicitly protects the technologies of connection and access to information, and it limits states’ ability to burden content originating abroad. The principles derived from Article 19 provide an important normative reorientation on individual rights for both domestic and international Internet governance debates.

Article 19’s guarantee of a right to the technologies of connection also fills a critical gap in human rights law. Protecting technology allows advocates to intervene in discussions about technological design that affect, but do not themselves violate, international human rights law. Failure to attend to these choices—to weigh in, ahead of time, on the human rights implications of software code, architecture design, and technological standards—can have significant consequences for human rights that may not be easily undone after the fact.

The Article also argues that technology companies are key partners in implementing Article 19. First, Article 19 directly binds these actors in some instances. Previously undiscovered portions of Article 19’s drafting history demonstrate that it does not have a state action requirement for dominant private actors. Second, as a pragmatic matter, technology companies can play an important role in enforcing Article 19 because of their central involvement in technology development and standard setting. Decisions about technology can make it easier or harder for states to violate international law, and technology companies should embed “human rights defaults” into their technology by designing it in ways that make it harder for states to violate international human rights.

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

## Introduction

The Internet has an international law problem. International institutions ranging from the International Telecommunication Union to the U.N. General Assembly are becoming increasingly involved in setting technological standards for the Internet. Apart from the question of the desirability of international regulation—which at this point may be an inevitability—this activity suffers from an even more fundamental defect. International regulation is proceeding without any attention to existing international law on freedom of expression or the consequences of these regulatory decisions for human rights. Without consideration of international human rights law and values, decisions about regulation will be driven by government and industry interests. The result is likely to be standards on issues such as data privacy and censorship that are inconsistent with international human rights law.

There are two reasons for the lack of attention to international law on freedom of expression. First, there has been surprisingly little development of this law. Although several U.N. human rights authorities recently have made extraordinarily valuable contributions toward articulating the scope and meaning of Article 19 in the online context,<sup>1</sup> this work has not gone far enough. Human rights law is much more robust than existing interpretive guidance would indicate, imposing duties on states and third parties with respect to the structure and governance of the Internet itself. Second, the values embedded in software code—both the instructions programmed into the software and hardware that makes technology work as well as the structure of that technology—tend to be invisible. Users perceive the constraints that software code imposes as a function of technology rather than the choices we make about technology. This invisibility makes it easy for states and industry to act in ways that mask the normative impact of their actions.

In this Article, I respond to both of these problems. This Article presents the first and only analysis of the meaning of Article 19 of the International Covenant on Civil and Political Rights (“ICCPR”)<sup>2</sup> as it applies to new technologies such as the Internet. Relying on a detailed examination of the drafting history of the ICCPR, I argue that, although the treaty does not guarantee a right to the “Internet” as such, it explicitly protects the “media” of expression and information and was intended to include after-arising technologies. This “media” clause, read together with the other provisions of Article 19(2), provides guidance for some of the most important Internet governance debates we face today. Article 19(2) guarantees rights to access technology, to seek information, and to remain anonymous online, and it limits states’ ability to burden foreign content. Indeed, for a document drafted over six decades ago, the ICCPR has a surprising amount to say about the Internet. The principles derived from Article 19(2) establish a foundation for an emerging “international law of the Internet” that provides an important normative reorientation on individual rights for both domestic and international Internet governance debates.

Protecting the technologies of connection is not merely a matter of semantics. First, having rights in the technology itself results in far more robust protection for human rights. This is particularly the case for Article 19, given the intimate relationship between speech and the means of

---

<sup>1</sup> See, e.g., Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*, Hum. Rts. Council, U.N. Doc. A/HRC/17/27 (May 16, 2011) [hereinafter “May 2011 La Rue Report”]; Hum. Rts. Comm., *General Comment No. 34 on Article 19: Freedoms of Expression and Opinion*, ¶15, U.N. Doc. CCPR/C/GC/34 (Sep. 12, 2011) [hereinafter, “General Comment No. 34”].

<sup>2</sup> International Covenant on Civil and Political Rights, art. 19(2), G.A. res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, entered into force Mar. 23, 1976 [hereinafter, “ICCPR”].

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

its expression. Limits on the means necessarily limit expression. Second, a right to the technologies of connection fills a critical gap in human rights law. There are many decisions about technological design that affect, but do not themselves violate, international human rights law. Protecting technology allows advocates to intervene in discussions about those decisions. Third, technology rights also serve as a framing device, orienting advocates on the effects of choices about technology on human rights. Failure to attend to these choices—to weigh in, ahead of time, on the human rights implications of software code, architecture design, and technological standards—can have significant consequences for human rights that may not be easily undone after the fact.

Finally, this Article turns to the question of implementation. With much of the Internet privately owned and operated, implementing an “international law of the Internet” might appear challenging, if not impossible. Relying on undiscovered portions of the drafting history of the ICCPR, I argue that Article 19 (in contrast to much of human rights law) does not have a state action requirement. Instead, it applies directly to the activities of private actors that substantially burden freedoms of expression and information. Non-state actors, to the extent that they interfere with the freedoms protected by Article 19(2), must justify their actions just as states would. Thus, Article 19(2) provides a basis for increased transparency and accountability for online intermediaries, including the development of digital due process standards.

We should not, however, view Internet service providers and other technology companies only, or even primarily, as threats to online speech. Instead, they are in some ways its greatest hope. Because they determine the development of the technology itself (the code and architecture of online expression and information) and often contribute to the development of standards that foster convergence on particular technologies, these companies are in a real position to influence the protection of online freedoms in tangible, significant, and immediate ways. Moreover, many of these companies have shown themselves willing to engage on issues of human rights, both out of a sense of moral obligation and because of their sensitivity to public pressure. In the final section of the Article, I call on technology companies to embed “human rights defaults” into their technology by designing it in ways that make it harder for states to violate international human rights.

Sections I and II of this Article outline the foundation of the international law of the Internet. Section I examines what Article 19(2) of the ICCPR says about technology, arguing that although the ICCPR does not protect the Internet *per se*, it does protect the “medium” of expression. I argue that a right to the technology of connection provides an important reorientation on the effect of technology on human rights and a basis for challenging decisions about technology that have human rights consequences but which do not themselves violate human rights. In Section II, I read the “media” clause in light of Article 19(2) as a whole to understand its meaning in the context of new technologies, arguing that it establishes rights of access to technology and information, a right to remain anonymous, and protection for foreign content. In Section III, I turn to the question of implementation, discussing the application of Article 19(2) on technology companies and calling on them to implement human rights defaults into the technology they build.

## **I. A Right to Media**

The Internet has recently been the focus of sustained international attention. International institutions ranging from the International Telecommunication Union to the U.N. General

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

Assembly are becoming increasingly involved in debates about the regulation of the Internet.<sup>3</sup> On issues ranging from cybersecurity to Internet peering, U.N. institutions are beginning to assert a role for themselves in Internet governance. The Internet is also being framed more explicitly than ever before as a human rights issue. A May 2011 report by the U.N. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, for example, was hailed—and criticized—as establishing a “human right to the Internet.”<sup>4</sup> The purpose of this section is to respond to these debates by considering whether existing international human rights law protects the technology of connection and, if so, the role such protection plays in guaranteeing international human rights.

### A. Internet As Right?

Until recently, with respect to online expression, international human rights law often seemed to be living in the past. In its 2009-2010 report, for example, the Human Rights Committee—the U.N. body charged with receiving reports about states’ compliance with the ICCPR—did not mention the Internet even in passing. In commenting on reports, it discussed freedom of expression only with respect to the rights of journalists, non-governmental organizations, human rights defenders, and “media professionals.”<sup>5</sup> Clearly, the Committee faces difficult choices about what address, and there are often very serious violations across a range of issues that require its attention. At the same time, for a right that “is not infrequently termed the core of the Covenant [on Civil and Political Rights] and the touchstone for all other rights guaranteed therein,”<sup>6</sup> it is striking that there is no mention in this report of the Internet or online expression, much less blogs, user-generated content, crowdsourcing, or social media.<sup>7</sup>

---

<sup>3</sup> See, e.g., MILTON L. MUELLER, NETWORKS AND STATES: THE GLOBAL POLITICS OF INTERNET GOVERNANCE (2010); TIM MAURER, CYBER NORM EMERGENCE AT THE UNITED NATIONS: AN ANALYSIS OF THE ACTIVITIES OF THE UN REGARDING CYBER-SECURITY 3 (2011); Patrick S. Ryan, *The ITU and the Internet's Titanic Moment*, 2012 STAN. TECH. L. REV. 8, 33 (2012); Nina Easton, *Where's the Outcry on the U.N. Push to Regulate the Internet?*, CNN MONEY (May 30, 2012). The proposed revisions to the ITU would not establish technical standards for the Internet (such as those promulgated by the Internet Engineering Task Force) but would instead create legal standards that would support and in some instances even mandate particular regulatory approaches to the Internet such as price discrimination. See, e.g., Center for Democracy and Technology, *ETNO Proposal Threatens to Impair Access to Open, Global Internet* 3, June 21, 2012.

<sup>4</sup> See, e.g., Jonathon Penney, *Internet Access Rights: A Brief History and Intellectual Origins*, 38 WM. MITCHELL L. REV. 10, 12 & n.6 (2011); *United Nations Report: Internet Access Is a Human Right*, L.A. TIMES, June 3, 2011; Vinton G. Cerf, *Internet Access Is Not A Human Right*, N.Y. TIMES, Jan. 4, 2012; Devin Coldewey, *Is the Internet a Human Right?*, TECHCRUNCH, Jan. 5, 2012.

<sup>5</sup> Rep. of the Hum. Rts. Comm'n, Aug. 1, 2009 – Jul. 31, 2010, U.N. Doc. A/65/40 (Vol. 1), at 28, 42, 43, 53, 66 & 79, GAOR, 65th Sess., Supp. No. 40 (2010) (responding to reports from Moldova, the Russian Federation, Mexico, Uzbekistan, and Israel).

<sup>6</sup> MANFRED NOWAK, U.N. COVENANT ON CIVIL AND POLITICAL RIGHTS: CCPR COMMENTARY 336 (1993).

<sup>7</sup> In its 2008-2009 report, the Committee does mention concern about retaliation against “users of non-conventional media,” Rep. of the Hum. Rts. Comm'n, Aug. 1, 2008 – Jul. 31, 2009, U.N. Doc. A/64/40 (Vol. 1), at 86, GAOR, 64th Sess., Supp. No. 40 (2009) (report on Azerbaijan), but otherwise focuses largely on journalists, the press, and traditional methods of political expression such as leafletting and canvassing, *id.* at 33 (canvassing and written materials in report on Japan), *id.* at 39 (human rights defenders in report on Nicaragua), *id.* at 43 & 48 (in a report on Spain, cautioning against the chilling effect of terrorism prosecutions and recommending that the country “guarantee freedom of expression for the press and the media, as well as for all citizens”), *id.* at 66 (journalists in Tanzania), *id.* at 79 (freedom of the press in Chad), *id.* at 85 (media, newspapers, radio in Azerbaijan).

*forthcoming 54 Harv. Int'l L.J.* \_\_ (2013)  
Please contact author for an updated version before quoting or citing.

With a series of reports by the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue,<sup>8</sup> and his predecessor, Abid Hussain,<sup>9</sup> a redrafting of the Committee's general comment on Article 19,<sup>10</sup> and two recent resolutions by the Human Rights Council,<sup>11</sup> the United Nations has been attempting to change all of that. In his May 2011 report, for example, Special Rapporteur addressed Internet filtering, graduated response laws, and Internet blackouts, asserting that in light of the importance of the Internet for human rights, that "facilitating access to the Internet for all individuals, with as little restriction to online content as possible, should be a priority for all States."<sup>12</sup> Similarly, the new and revised *General Comment No. 34* takes a close look at online media, noting that "States parties should take all necessary steps to foster the independence of these new media and to ensure access of individuals thereto."<sup>13</sup> The June 2012 resolution of the Human Rights Council calls on states "to promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries."<sup>14</sup>

Special Rapporteur La Rue's statements have generated significant debate, with many even characterizing his May 2011 report as proclaiming a "human right to the Internet."<sup>15</sup> In reality, the Special Rapporteur has been drawing much finer distinctions in his reports. He has emphasized the importance of access to the Internet for both freedom of expression and other human rights and

---

<sup>8</sup> 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*, ¶ 61, U.N. Doc. A/66/290 (Aug. 10, 2011) [hereinafter "August 2011 La Rue Report"]; May 2011 La Rue Report, *supra* note 1; Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*, Hum. Rts. Council, U.N. Doc. A/HRC/14/23 (Apr. 20, 2010) [hereinafter "2010 La Rue Report"]. The Special Rapporteur has also considered access to the Internet extensively in his individual country studies. See, e.g., Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Mission to Algeria*, ¶¶ 63-71, 105-106, Hum. Rts. Council, U.N. Doc. A/HRC/20/17/Add.1 (June 12, 2012).

<sup>9</sup> See, e.g., Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Mr. Abid Hussain*, ¶¶ 29-43, Hum. Rts. Council, U.N. Doc. E/CN.4/2006/55 (Dec. 30, 2005); Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Mr. Abid Hussain*, ¶¶ 88-95, Hum. Rts. Council, U.N. Doc. E/CN.4/2002/75 (Jan. 30, 2002); Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Mr. Abid Hussain*, ¶¶ 57-69, Hum. Rts. Council, U.N. Doc. E/CN.4/2001/64 (Feb. 13, 2001); Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Mr. Abid Hussain*, ¶¶ 54-58, Hum. Rts. Council, U.N. Doc. E/CN.4/2000/63 (Jan. 18, 2000); Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Mr. Abid Hussain*, ¶¶ 29-36, Hum. Rts. Council, U.N. Doc. E/CN.4/1999/64 (Jan. 29, 1999)

<sup>10</sup> General Comment No. 34, *supra* note 1, ¶ 15.

<sup>11</sup> Human Rights Council Res. 20, The Promotion, Protection and Enjoyment of Human Rights on the Internet, ¶ 3, 20th Sess., June 29, 2012, U.N. Doc. A/HRC/20/L13 [hereinafter "H.R.C. Res. 20"]; Human Rights Council Res. 12/16, Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development, 12th Sess., Oct. 12, 2009, U.N. Doc. A/HRC/RES/12/16 [hereinafter "H.R.C. Res. 12/16"]. The Human Rights Council replaced the Commission on Human Rights in March 2006. See G.A. Res. 60/251, 60th Sess., U.N. Doc. A/RES/60/251 (Apr. 3, 2006).

<sup>12</sup> May 2011 La Rue Report, *supra* note 1, ¶ 2.

<sup>13</sup> General Comment No. 34, *supra* note 1, ¶ 15.

<sup>14</sup> H.R.C. Res. 20, *supra* note 11, ¶ 3.

<sup>15</sup> See, e.g., Penney, *supra* note 4, at 12 & n.6.

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

condemned certain practices that “cut off access to the Internet entirely” as “disproportionate” and in violation of Article 19.<sup>16</sup> A joint declaration signed by a group of special rapporteurs on freedom of expression noted that “Freedom of expression applies to the Internet, as it does to all means of communication.”<sup>17</sup> Special Rapporteur La Rue has not said, however, that there is a right to the Internet itself, as he has since noted in both subsequent public appearances<sup>18</sup> and in his reports.<sup>19</sup> In his August 2011 report, he clarified that states were obligated to promote the means necessary to exercise the right to freedom of expression and that such means included the Internet, but that there was no right to the Internet “as such.”<sup>20</sup>

Popular characterizations of the Special Rapporteur’s May 2011 report as declaring a “right to the Internet” have sparked compelling debates about the relationship between human rights and new technologies. Vince Cerf, one of the “fathers of the Internet,” argued in a New York Times opinion piece that “technology is an enabler of rights, not a right itself.”<sup>21</sup> He maintained that it would be wrong to declare the Internet a human right because:

There is a high bar for something to be considered a human right. Loosely put, it must be among the things we as humans need to live healthy, meaningful lives, like freedom from torture or freedom of conscience. It is a mistake to place any particular technology in this exalted category, since over time we will end up valuing the wrong things.<sup>22</sup>

Cerf raises important points. Our inability to predict technological developments and the role these developments will play with respect to human rights should lead us to be particularly cautious about immortalizing any particular kind of technology in international law. Further, recognizing a new right to the Internet would raise concerns about the undue expansion of international human rights law. Philip Alston has cautioned that “a proliferation of new rights would be much more likely to contribute to a serious devaluation of the human rights currency than to enrich significantly the overall coverage provided by existing rights.”<sup>23</sup> Among other things, recognizing a “new” right to the Internet would lead to calls to recognize rights in other specific technologies and might potentially weaken the protections for freedom of expression in general.

There is no need for concern about recognizing new rights, however, because international law already protects the Internet. Although states are increasingly declaring Internet access to be a fundamental right under domestic law, state practice in this area is not consistent or widespread enough to constitute a rule of customary law.<sup>24</sup> (Although one might, of course, point to laws in

---

<sup>16</sup> May 2011 La Rue Report, *supra* note 1, ¶ 69(4).

<sup>17</sup> *Joint Declaration on Freedom of Expression and the Internet*, June 1, 2011, ¶ 1a [hereinafter, “Joint Declaration”]. The declaration was signed by UN Special Rapporteur Frank La Rue, OSCE Representative on Freedom of the Media Dunja Mijatović, OAS Special Rapporteur on Freedom of Expression Catalina Botero Marino, and ACHPR Special Rapporteur on Freedom of Expression and Access to Information Faith Pansy Tlakula.

<sup>18</sup> Frank LaRue, Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Remarks at the Global Congress on Intellectual Property and the Public Interest (Aug. 26, 2011).

<sup>19</sup> August 2011 La Rue Report, *supra* note 8, ¶ 61.

<sup>20</sup> *Id.*

<sup>21</sup> Cerf, *supra* note 4.

<sup>22</sup> *Id.*

<sup>23</sup> Philip Alston, *Conjuring Up New Human Rights: A Proposal for Quality Control*, 78 AM. J. INT’L L. 607, 614 (1984).

<sup>24</sup> See MARK WESTON JANIS, *INTERNATIONAL LAW* 48 (6th ed., 2012) (describing the requirements for a rule of customary international law).



*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

Finland and Estonia or the decision by Costa Rica's Constitutional Court establishing access to the Internet as a fundamental right<sup>25</sup> as evidence of an emerging rule.) Article 19(2) of the ICCPR, however, provides an international law basis for protecting the technologies of connection. Article 19(2) of the ICCPR guarantees the “freedom to seek, receive and impart information and ideas . . . through any other media of his choice.”<sup>26</sup> As the next part will demonstrate, this “media clause” protects both the form and the means of expression and was explicitly intended to apply to after-arising technologies.

## B. The “Media” Clause

Article 19(2) of the ICCPR protects not only expression, but also its medium. Article 19(2) guarantees the right to seek, receive, and impart information and ideas “either orally, in writing or in print, in the form of art, or *through any other media of his choice.*”<sup>27</sup> The key term in Article 19(2) is “media.” Does it include the Internet? Under Article 31(1) of the Vienna Convention on the Law of Treaties, which is understood by the International Court of Justice to constitute customary international law on the interpretation of treaties,<sup>28</sup> a treaty is to be interpreted “in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose.”<sup>29</sup> Thus, the first step toward understanding the scope of Article 19(2) is to consider the ordinary meaning of the text in context.

Using a textual approach, the term “media” possesses two possible meanings, referring potentially both to the channel and to the form of expression. Media can be “the means of communication, as radio and television, newspapers, and magazines, that reach or influence people widely.”<sup>30</sup> It can also serve as the plural form of “medium,” which refers both to the “means or agency for communicating or diffusing information, news, etc.” and “the category of” and “materials used in a work of art.”<sup>31</sup> Subsequent commentators appear to have read Article 19(2) in this manner, to refer both to the channel and the form of communication, noting that it protects not only verbal communication but also “all media of acoustic, visual, electronic and other communication,” including “radio and television, electronic media, film, photography, music, graphic and other arts, etc.”<sup>32</sup> Similarly, in its revised *General Comment No. 34*, the Human Rights

<sup>25</sup> See, e.g., *Internet Access Is a “Fundamental Right,”* BBC NEWS (Mar. 8, 2010, 08:52 GMT), <http://news.bbc.co.uk/2/hi/8548190.stm>; Renata Avila, *Costa Rica: Cybercrime Law Threatens Internet Freedom*, GLOBAL VOICES ADVOCACY: DEFENDING FREE SPEECH ONLINE (July 20, 2012, 18:38 GMT), <http://advocacy.globalvoicesonline.org/2012/07/20/costa-rica-cybercrime-law-threatens-internet-freedom/>. In France, the *Conseil Constitutionnel* also struck down as unconstitutional the first version of a law that would have given the government the ability to shut down access to the Internet for individuals found to have repeatedly violated the copyright rights of others, although it did not recognize an explicit right to the Internet in the process. See Nicola Lucchi, *Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression*, 19 CARDOZO J. INT'L & COMP. L. \_\_, \_\_ (2011).

<sup>26</sup> ICCPR, *supra* note 2, art. 19(2).

<sup>27</sup> *Id.* (emphasis added).

<sup>28</sup> ANTHONY AUST, *MODERN TREATY LAW AND PRACTICE* 232 (2d ed. 2007).

<sup>29</sup> Vienna Convention on the Law of Treaties, art. 31(1), 1155 U.N.T.S. 331, 8 I.L.M. 679, *entered into force* Jan. 27, 1980 [hereinafter “VCLT”].

<sup>30</sup> *Media*, DICTIONARY.COM, <http://dictionary.reference.com/browse/media?s=t&ld=1089>.

<sup>31</sup> *Medium*, DICTIONARY.COM, <http://dictionary.reference.com/browse/medium?s=t>.

<sup>32</sup> NOWAK, *supra* note 6, at 342; see also Dr. Agnes Callamard, Keynote Speech: For a Rights-Based Approach to Wireless Technology and Digital Dividend (May 2008) (text available at [http://www.article19.org/data/files/08\\_05\\_03\\_CONFERENCE\\_Wireless\\_digital\\_dividend.pdf](http://www.article19.org/data/files/08_05_03_CONFERENCE_Wireless_digital_dividend.pdf)) (arguing that the

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

Committee also read Article 19(2) as protecting “all forms of expression and the means of their dissemination,” noting that “[m]eans of expression include books, newspapers, pamphlets, posters, banners, dress and legal submissions” as well as “all forms of audio-visual as well as electronic and internet-based modes of expression.”<sup>33</sup>

The context of the “media” clause in Article 19(2) also indicates that “media” protects both the form and channel of communication. The media clause takes the form of a list: “either orally, in writing or in print, in the form of art, or through any other media of his choice.” The use of the word “other” indicates that what precedes the term “media” are intended as examples. The rule of *ejusdem generis* as a principle of treaty interpretation provides that, “When general words follow special words, the general words are limited by the *genus* (class) indicated by the special words.”<sup>34</sup> These special words—“orally,” “in writing,” “in print,” and “in the form of art”—refer both to the forms and channels of expression. “Orally,” “in writing” and “in the form of art” are forms of expression; “in print,” contrasted as it is with “in writing,” refers to print media. Thus, the term media, as defined by the preceding specific words in the list, includes both the form and the channel of expression.

The preparatory materials for the articles on freedom of expression and information in the ICCPR as well as the Universal Declaration of Human Rights (“UDHR”)<sup>35</sup> confirm this meaning. Article 32 of the Vienna Convention offers, as “supplementary means of interpretation,” recourse to the treaty’s preparatory work (or *travaux préparatoires*) and the circumstances of the treaty’s conclusion, either “to confirm the meaning” that results from applying the foregoing principles, or “to determine the meaning when the interpretation according to article 31: (a) leaves the meaning ambiguous or obscure; or (b) leads to a result which is manifestly absurd or unreasonable.”<sup>36</sup> Because the term “media” is susceptible to multiple interpretations, resort to preparatory works is appropriate.

The earliest versions of Article 19(2) included protection for both forms and channels of communication. The text of Article 19 of the ICCPR<sup>37</sup> was prepared together with the text of the corresponding article on freedom of expression and information for the UDHR. The earliest two

---

expression “through any media” “is not limited to traditional media such as newspapers or radio, but also covers any contemporary or future technology used for the exchange of ideas and information, including wireless communication devices”).

<sup>33</sup> General Comment No. 34, *supra* note 1, ¶ 12.

<sup>34</sup> AUST, *supra* note 28, at 249.

<sup>35</sup> The negotiation of Article 19 of the UDHR can be considered in interpreting the scope of Article 19 of the ICCPR. Although there is no definitive answer to what constitutes preparatory work, as a general matter, it can include anything “characterized as ‘illuminating a common understanding.’” RICHARD K. GARDINER, TREATY INTERPRETATION 100 (2008). The negotiation of Article 19 of the UDHR illuminates the parties’ shared understanding of the equivalent article in the ICCPR because the foundational texts for both articles were drafted by the same body, the Conference on Freedom of Information, and contained many of the same elements and terms. Further, the International Court of Justice has itself considered not only a predecessor treaty but also a “more remote bilateral source” in tracing the historical evolution of particular treaty language. *See id.* at 101 (citation omitted).

<sup>36</sup> VCLT, *supra* note 29, art. 32.

<sup>37</sup> The ICCPR was not called by this name during the negotiations. Negotiations initially focused on drafting articles for a single convention, and it was only later in the process that the convention articles were divided among two treaties, the ICCPR and its companion, the International Covenant on Economic, Social and Cultural Rights (“ICESCR”), International Covenant on Economic, Social and Cultural Rights, G.A. res. 2200A (XXI), 21 U.N.GAOR Supp. (No. 16) at 49, U.N. Doc. A/6316 (1966), 993 U.N.T.S. 3, *entered into force* Jan. 3, 1976. *See* Preparing of Two Draft International Covenants on Human Rights, G.A. Res. 543, U.N. GAOR, 6th Sess., 375th mtg. at 8, U.N.Doc. A/2119 (1952). This Article refers to the convention by its later name, the ICCPR.

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

drafts for both documents were a “Secretariat Draft”<sup>38</sup> and a revision thereof, the “Drafting Committee Draft.”<sup>39</sup> The Secretariat Draft of the UDHR provided for “freedom of speech and of expression and by any means whatsoever” and guaranteed “reasonable access to all channels of communication.”<sup>40</sup> Although “means” and “channel” are enumerated separately, the Drafting Committee Draft, which was intended to encompass the Secretariat Draft,<sup>41</sup> added to this text by providing examples of “means” that include both forms and channels: “There shall be freedom of expression either by word, in writing, in the press, in books, or by visual, auditive or other means. There shall be equal access to all channels of communication.”<sup>42</sup>

The Drafting Committee Draft was sent to the Sub-Commission on Freedom of Information and of the Press for its consideration. The Sub-Commission proposed draft articles that formed the basis of discussions at a Conference on Freedom of Information in 1948. The Final Act of the Conference (“Conference Draft”) was a key text on which all subsequent discussions were based.<sup>43</sup> It was the third and final of the drafts of the text for the UDHR. The Conference Draft text for the UDHR eliminated the examples added by the Drafting Committee and returned to the phrasing of the Secretariat Draft of “by any means.”<sup>44</sup> Thus, the Conference Draft for the UDHR read: “Everyone shall have the right to freedom of thought and expression; this right shall include freedom to hold opinions without interference and to seek, receive and impart information and ideas by any means and regardless of frontiers.”<sup>45</sup>

The meaning of the term “means” to refer to both the form and channel of communication was further confirmed when the Human Rights Committee changed “means” to “media.” Although this change narrowed the scope of the text, it did so only to conform the text to the intentions of the drafters to extend protection to the form and channel of communication. During the debates, a representative of the Coordinating Board of Jewish Organizations called attention to the danger of the phrase, “by any means,” noting that although these words “might refer simply to the technical media of imparting information,” there was a risk that it might be used to justify “incitement to hatred and violence against racial or religious groups.”<sup>46</sup> Describing the change as “superfluous,” the Chinese delegate suggested the phrasing “through all media of expression” in order to respond to this concern, and the remaining delegates agreed.<sup>47</sup> The U.K. delegate made clear this was a change

---

<sup>38</sup> Comm’n on Hum. Rts., Draft Outline of International Bill of Rights, U.N. Doc. E/CN.4/AC.1/3 (Jun. 4, 1947) [hereinafter “Secretariat Draft”].

<sup>39</sup> Comm’n on Hum. Rts., Rep. of the Drafting Comm. to the Comm’n on Hum. Rts., Annexes F & G, U.N. Doc. E/CN.4/21 (Jul. 1, 1947) [hereinafter “Drafting Committee Draft”].

<sup>40</sup> Secretariat Draft, *supra* note 38; *see also* John P. Humphrey, *The Freedoms of Opinion and Expression (Freedom of Information)*, in HUMAN RIGHTS IN INTERNATIONAL LAW: LEGAL AND POLICY ISSUES 181, 183-84 (Theodor Meron ed. 1984).

<sup>41</sup> Humphrey, *supra* note 40, at 184.

<sup>42</sup> Drafting Committee Draft, *supra* note 39.

<sup>43</sup> U.N. Secretary-General, *Opinion of the United Nations Conference on Freedom of Information on Articles 17 and 18 of the Draft International Declaration on Human Rights and Article 17 of the Draft International Covenant on Human Rights*, at 2, U.N. Doc. E/CN.4/84 (Apr. 30, 1948) [hereinafter “Conference Draft”]; *see also Summary of the Work of the Drafting Comm. to the Comm’n on Human Rights*, 1948 YB on Hum. Rts. 457, 475. Although the Conference Draft proposal for the ICCPR was presented as one of three options, together with proposals by France and the Union of Soviet Socialist Republics (“USSR”), the Conference Draft formed the basis of subsequent discussion. Rep. of the Comm’n on Human Rights, 3rd Sess., May 27-June 18, 1948, at 28-29, U.N. Doc. E/800 (June 28, 1948).

<sup>44</sup> Conference Draft, *supra* note 43.

<sup>45</sup> *Id.* at 2.

<sup>46</sup> Comm’n on Hum. Rts., 3d Sess., 62d mtg, at 13, U.N. Doc. E/CN.4/SR.62 (Jun. 11, 1948).

<sup>47</sup> Comm’n on Hum. Rts., 3d Sess., 63d mtg, at 5, 12-13, U.N. Doc. E/CN.4/SR.63 (Jun. 11, 1948).

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

in order to “clarify a meaning which might have been ambiguous in the original wording.”<sup>48</sup> Thus, the Commission changed “by any means” to “through any media” in order to make clear what had been the intent all along, that the article protected both the form and the channel of communication, and was not a license to use “means” such as violence. The new text of the article on freedom of expression for the UDHR was renumbered as Article 19, and the General Assembly adopted it by a vote of 44-7, with two abstentions, on September 24, 1948.<sup>49</sup>

Early drafts of the ICCPR also specified particular channels and forms of expression, thus indicating that the later decision to replace these with the term “media,” without any intent to narrow, included both channel and form. The Drafting Committee Draft of the text for the ICCPR protected the right to express and publish ideas “orally, in writing, in the form of art, or otherwise” (i.e., the form of communication) and to receive and disseminate information “by books, newspapers, or oral instruction, and by the medium of all lawfully operated devices”<sup>50</sup> (i.e., the channel of communication). The Conference Draft for the ICCPR combined these two types of protection into a single phrase, “either orally, or by written or printed matter, in the form of art, or by legally operated visual or auditory devices.”<sup>51</sup> The United States, which had tended throughout the negotiations over the ICCPR (then generally referred to as the Covenant) to push for more general language, especially in the limitations clause of Article 19,<sup>52</sup> proposed a fourth version of the ICCPR text (the “U.S. Draft”) that further condensed this to its near final form, “either orally, in writing or in print, in the form of art, or through any other media.”<sup>53</sup>

The delegates debated and eventually adopted the more general phrase of “through any other media” instead of a more specific enumeration of “devices,” making clear the general phrase was intended to include the channel of communication. In negotiations over the U.S. Draft in the Sixth Session of the Human Rights Committee, where most of the revision of Article 19 took place,<sup>54</sup> the United Kingdom advocated for the more specific phrase, “by legally operated visual or auditory devices” in order to safeguard its ability to engage in governmental licensing of radio and television.<sup>55</sup> Other delegates felt the U.K. text was too “restrictive” and that the issue of licensing would be better addressed in the limitations clause of Article 19(3).<sup>56</sup> The U.K. amendment was withdrawn and the text eventually adopted was the phrase “or other media.”<sup>57</sup> The Secretary

---

<sup>48</sup> *Id.* at 12.

<sup>49</sup> Summary of the Work of the General Assembly, 1948 Y.B. on Hum. Rts. 465, 465.

<sup>50</sup> Drafting Committee Draft, *supra* note 39; *see also* MARC J. BOSSUYT, GUIDE TO THE “TRAVAUX PRÉPARATOIRES” OF THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS 373 (1987).

<sup>51</sup> Conference Draft, *supra* note 43.

<sup>52</sup> *See e.g.*, MARGARET A. BLANCHARD, EXPORTING THE FIRST AMENDMENT: THE PRESS-GOVERNMENT CRUSADE OF 1945-1952, 187 (1986).

<sup>53</sup> United States, *Revised Text of the United States Proposal for Art. 17*, U.N. Doc. E/CN.4/433/Rev.2 (Apr. 20, 1950) [hereinafter “U.S. Draft”]; *see also* Comm’n on Hum. Rts. Summ. Record, 6th Sess., 163d mtg., at 13, U.N. Doc. E/CN.4/SR.163 (May 2, 1950) [hereinafter “Summary Record No. 163”] (adopting U.S. Draft as baseline text).

<sup>54</sup> Although later discussions in the Commission revisited some of the ground covered in the Sixth Session, the text of the article that emerged from the Sixth Session (then labeled as Article 14) was substantially the same as the text eventually incorporated into the ICCPR as Article 19. Rep. of the Comm’n on Hum. Rts., 6th Sess., Mar. 27 – May 19, 1950, U.N. Doc. E/1681, GAOR 11th Sess., Supp. No. 5 (1950).

<sup>55</sup> *See, e.g.*, United Kingdom, Amendments to Text Proposed for Article 17 in E/CN.4/433/Rev.2, U.N. Doc. E/CN.4/440 (April 20, 1950); Comm’n of Hum. Rts. Summ. Record, 8th Sess., 320 mtg., at 5, U.N. Doc. E/CN.4/SR.320 (Jun. 18, 1952) [hereinafter “Summary Record No. 320”].

<sup>56</sup> Comm’n on Hum. Rts. Summ. Rec., 6th Sess., ¶ 53, U.N. Doc. E/CN.4/SR.165 (May 2, 1950) [hereinafter “Summary Record No. 165”].

<sup>57</sup> *Id.* ¶ 64.

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

General, in transmitting the draft of the Eighth Session of the Commission on Human Rights to the General Assembly for discussion, noted that the U.K. formulation was rejected precisely because it was feared that it “might throttle channels of communication.”<sup>58</sup>

### C. After-Arising Technology

The text and drafting history of the ICCPR also demonstrate that the negotiating states intended the term “media” to encompass not just the particular channels of communication available at the time (e.g., newspapers and increasingly radio and television) but also technology that had yet to be invented. It is appropriate to interpret a treaty term in light of current facts if the parties intended the interpretation of the term to evolve over time.<sup>59</sup> An evolutive approach that takes account of the facts as they exist at the time of the treaty’s interpretation is particularly appropriate for human rights treaties if necessary in order to ensure fulfillment of the treaty’s object and purpose of protecting individual rights.<sup>60</sup>

The party’s intention that the term “media” evolve over time and be interpreted with reference to current facts is clear from the text itself. The parties chose to use the general term “media” instead of more specific terms referring to particular technologies. Further, an evolutive approach is especially appropriate when the parties use terms referencing concepts in fields that evolve over time, such as scientific fields. As Julian Arato explains, “It may be assumed, for example, that by using a scientific term the parties did not intend to fix its meaning and thereby potentially ground their future obligations on outmoded or falsified scientific concepts, but intended these terms to connote obligations keyed to the evolving meaning of those expressions.”<sup>61</sup> Although the term “media” is a technical not scientific term, a similar approach is warranted. It may be assumed that the parties did not intend the meaning of this term to be fixed in time, protecting only the channels of communication available at the time of drafting. Such an approach would have rendered this part of Article 19(2) obsolete relatively quickly, as the pace of technological development transformed information and communication technologies in ways that could not have been contemplated in the early 1950s. It can be assumed that the drafters of a document designed to articulate and create an effective framework for protecting individual rights<sup>62</sup> would not have intended for any part of this treaty to become so quickly obsolete.

Further, the drafting history and circumstances of the treaty’s drafting provides clear evidence that the drafters intended it to include after-arising technology. In discussions in the Sixth

<sup>58</sup> U.N. Secretary General, *Annotations on the Text of the Draft International Covenants on Human Rights*, ¶ 137, U.N. Doc. A/2929 (July 1, 1955) [hereinafter, “Annotations”]; see also BOSSUYT, *supra* note 50, at 383

<sup>59</sup> See, e.g., GARDINER, *supra* note 35, at 172 (citing application of the “generic” doctrine in *Aegean Sea Continental Shelf*, [1978] ICJ Reports, at 32, para. 77); Pierre-Marie Dupuy, *Evolutionary Interpretation of Treaties: Between Memory and Prophecy*, in *THE LAW OF TREATIES BEYOND THE VIENNA CONVENTION* 122, 131 (Enzo Cannizzaro ed. 2011) (citing application of the “generic” doctrine in *Case Concerning the Dispute Regarding Navigational and Related Rights (Costa Rica v. Nicaragua)*, Judgment of 13 July 2009, paras. 66-67); see generally Dupuy, *supra* note 59, at 131.

<sup>60</sup> Rudolf Bernhardt, *Evolutionary Treaty Interpretation, Especially of the European Convention on Human Rights*, 42 GERMAN Y.B. INT’L L. 11, 23 (1999).

<sup>61</sup> Julian Arato, *Subsequent Practice and Evolutive Interpretation: Techniques of Treaty Interpretation Over Time and Their Diverse Consequences*, 9 L. & PRACTICE INT’L COURTS & TRIBUNALS 443, 469 (2010).

<sup>62</sup> See Human Rights Committee, *General Comment No. 24: Issues Relating to Reservations Made upon Ratification or Accession to the Covenant or the Optional Protocols Thereto, or in Relation to Declarations Under Article 41 of the Covenant*, U.N. Doc. CCPR/C/21/Rev.1/Add.6 (1994), para. 7 (describing the object and purpose of the treaty as “to create legally binding standards for human rights by defining certain civil and political rights and placing them in a framework of obligations which are legally binding for those States which ratify”).

*forthcoming 54 Harv. Int'l L.J.* \_\_ (2013)  
Please contact author for an updated version before quoting or citing.

Session, the delegate from France, supported by the delegate from Belgium, argued against the U.K. phrasing of “by legally operated visual or auditory devices” on the ground that “[t]he members of the Commission must take into account the fact that their work concerned the future and not the past; no one could foresee what information media would be employed in a hundred years’ time.”<sup>63</sup> This is confirmed by historical accounts of the U.S. position in leading the effort to protect freedom of expression under international law. Margaret Blanchard, in her study of the U.S. campaign for international freedom expression in the post-WWII era, notes that even at the outset of international negotiations, the U.S. State Department had made clear that it was interested

in promoting freedom for all existing media—newspapers, news agencies, newsreels, radio, magazines, books, and motion pictures—rather than just for newspapers and news agencies. The department was also worried about the physical facilities of communications—cables and radio transmitters, for instance. The inclusiveness of the department’s list of information-related topics was forward-looking, for in the mid-1940s, newspapers and news agencies considered themselves as almost the sole organs of information.<sup>64</sup>

Clearly, Article 19(2) does not explicitly protect the Internet, nor could the delegates have done so as a part of the negotiations of the ICCPR in the early 1950s. The drafting history and circumstances of its conclusion demonstrate, however, that they intended the “media” clause to sweep as broadly as possible and to include protection for channels of communication not yet contemplated.

Thus far, the text and drafting history of Article 19(2) have made three things clear: It extends protection to “media,” media includes the channel of expression, and “media” or channel must be understood in terms of the factual conditions existing at the time of interpretation. What precisely, however, does “media” include in light of today’s information and communication technology landscape? The range of potentially relevant technologies and services is staggering: It might include, for example, the actual hardware of communication (e.g., computers, modems, cables), the software that makes this hardware work (e.g., Outlook, Safari, or Firefox), the protocols that render these systems compatible with one another (e.g., TCP/IP, WiFi), the networks that connect computers to one another (e.g., the Internet, local intranets), the platforms that are built on top of the networks (e.g., Facebook, Twitter), and the services that make this all run (e.g., broadband providers, web hosting services). Does all of this constitute “media”?

The ICCPR purposefully, and wisely, refuses to answer this question with specifics. The meaning of the “media” clause and what it requires not only will change over time, but also will vary depending on the context, location and infrastructure. For example, in places that lack the necessary communications infrastructure (such as the actual physical cables necessary to connect to the Internet), the available medium of expression and information sharing might not be the Internet but rather mobile phones.<sup>65</sup> In other places, radio might be the most effective and practical way of sharing information.<sup>66</sup> Because it is framed generally without naming particular technologies, Article

---

<sup>63</sup> Summary Record No. 165, *supra* note 56, ¶ 54.

<sup>64</sup> BLANCHARD, *supra* note 52, at 28 .

<sup>65</sup> See August 2011 La Rue Report, *supra* note 8, ¶¶ 67, 76; Tom Sarrazin, *Texting, Tweeting, Mobile Internet: New Platforms for Democratic Debate in Africa*, FESMEDIA AFRICA SERIES 1, 17 (2011), available at <http://library.fes.de/pdf-files/bueros/africa-media/08343.pdf>.

<sup>66</sup> For example, a women-run community-based development project in Southeast Kenya chose to disseminate information via radio instead of cell phones because of lack of cellular coverage and women’s concerns that their

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

19(2) is flexible enough to support claims to whatever medium is most appropriate for the particular local infrastructure and information needs.

Article 19(2) does, however, provide some guidance with respect to the outer boundaries of the term “media.” Article 19(2) protects the “freedom to seek, receive and impart information and ideas . . . through any other media of his choice.” Thus, “media” necessarily must be something that individuals can use to engage in these activities—to seek, to receive, and to impart. The right to seek information is a right “*actively* to seek information, which goes beyond mere passive reception.”<sup>67</sup> Receiving and imparting are interactive in nature, activities by which individuals connect with others to share information and ideas. “Media” might therefore be understood as any technology that allows individuals to connect with information and expression and with one another. In this way, the “media” clause of Article 19(2) provides a strong foundation for the “freedom to connect” that Secretary of State Clinton articulated in her speech in January of 2010. Clinton argued that there was an additional freedom that flowed from and was inherent in the freedoms identified by President Franklin Roosevelt in his 1941 Four Freedoms speech. This inherent freedom, a “freedom to connect,” is based on “the idea that governments should not prevent people from connecting to the internet, to websites, or to each other.”<sup>68</sup> Although a “freedom to connect” is not located explicitly in Article 19(2), it is supported by both the protection of the rights to seek, receive and impart information as well as protection of the technologies required for these activities.

The “media” clause of Article 19(2) protects any technology that facilitates connection. As such, it certainly protects the Internet, one of the most effective means for seeking out information and ideas and connecting with others. Indeed, even platforms like Facebook and Twitter, which certainly facilitate connection, would fall within the scope of “media” under Article 19(2). This does not mean that individuals would have the same rights with respect to each of these technologies (i.e., there may be a right to access the Internet but not Facebook). As discussed in more detail below, the scope of the right will depend on context and the role played by the particular technology in facilitating freedom of expression and information. This article uses the phrase “technologies of connection” to refer broadly to all of the media that facilitate connection and thus are protected under Article 19(2).

It is possible, however, that some new information and communication technologies might be so different in kind from the “media” available at the time of the drafting of the ICCPR that they should not be understood to be encompassed within the term “media.” There are two changes associated with the rise of new information and communication technologies that make the harms of the Internet greater than were present at the time of the drafting, and thus potentially affect our understanding of the drafter’s intentions in protecting technology. First, there is the problem of quantity. In many ways, the Internet’s primary difference over older technologies is one of scale, not kind; it simply enables far more communication among more people for lower cost than ever before. In some instances, however, differences in scale can become differences in kind. Advertising through traditional mail is held in check in part because of the cost of postage. When that cost drops radically, as is the case with email, there is more solicitation, and the resulting phenomenon—spam—becomes a problem unlike any other. Exponential increases in the ability to invade

---

husbands would take and sell a cell phone. S. Revi Sterling, *AIR: Advancement through Interactive Radio*, at 4 (2007), available at <http://www.cs.colorado.edu/departments/publications/reports/docs/CU-CS-1006-06.pdf>.

<sup>67</sup> NOWAK, *supra* note 6, at 343.

<sup>68</sup> Secretary of State Hillary Rodham Clinton, Remarks on Internet Freedom, Jan. 21, 2010.

*forthcoming 54 Harv. Int'l L.J.* \_\_ (2013)  
Please contact author for an updated version before quoting or citing.

someone's privacy or defame their reputation may be a qualitative and not just a quantitative difference over past technologies.<sup>69</sup>

Second, new technologies often lack filters. At the time of the drafting of the ICCPR, the available information and communication technologies included newspapers, radio, television, telephone, and telegraph. The communication patterns of these media were either one to many (i.e., newspapers, radio, television) or one to one (i.e., telephone, telegraph). Broadcasts to an audience (one to many) were largely moderated; newspapers and radio broadcasters functioned as filters by choosing what and how to publish. The current information and communication environment, however, supports a many to many model in which anyone can be a producer of expression and information.<sup>70</sup> As Special Rapporteur La Rue notes, "with the advent of Web 2.0 services, or intermediary platforms that facilitate participatory information sharing and collaboration in the creation of content, individuals are no longer passive recipients, but also active publishers of information."<sup>71</sup> Blogs and platforms such as Facebook and Twitter enable any individual to broadcast his or her message to an audience without the mediating influence of a publisher.<sup>72</sup> This democratization of access has been augmented by technological developments (such as mobile phone penetration, broadband, and digitization) that have made access to the means for sharing information and communication far more widespread than ever before.<sup>73</sup>

Because of the exponential increase in communication volume enabled by new technologies and the lack of filters for this communication, new technologies enable far more harmful expression than was possible at the time of the ICCPR's drafting. It is possible that the drafters might not have wanted to protect the technologies of connection in light of these risks. There are several reasons, however, to believe they would have included these new technologies despite the risk of greater and unanticipated harm. First, the drafters intended Article 19(2) to apply to individuals, not just professionals. The text provides that the rights of Article 19 are guaranteed to "[e]veryone."<sup>74</sup> During negotiations, the U.S. delegate emphasized that freedom of expression and information were simply about freedom of the press; rather, this was about "freedom of inquiry and teaching, to freedom of artistic expression, to the rights of every person to gain information from any source."<sup>75</sup> In discussing a ban on war propaganda, the Chinese delegate to the Third Committee emphasized that "it should not be forgotten that article 19 of the draft Covenant did not apply solely to journalists but, as did all the other articles, to every individual as a human being."<sup>76</sup> The drafting of

---

<sup>69</sup> See Matthew Sag, *Copyright and Copy-Reliant Technology*, 103 NW. U. L. REV. 1607, 1612 (2009); P.W. Anderson, *More Is Different: Broken Symmetry and the Nature of the Hierarchical Structure of Science*, 177 SCIENCE 939 (1972).

<sup>70</sup> Clay Shirky, *Communities, Audiences, and Scale*, SHIRKY.COM (Apr. 6, 2002), [http://shirky.com/writings/community\\_scale.html](http://shirky.com/writings/community_scale.html).

<sup>71</sup> May 2011 La Rue Report, *supra* note 1, ¶ 19; see also Global Internet Liberty Campaign, "Regardless of Frontiers": Protecting the Human Right to Freedom of Expression on the Global Internet, at 5 ("The concept of a right to 'impart information takes on new meaning when anyone can be a publisher.'").

<sup>72</sup> See, e.g., Dan Hunter & F. Gregory Lastowka, 46 WM. & MARY L. REV. 951, 983-84 (2004).

<sup>73</sup> See MOLLY LAND ET AL., ICT4HR: INFORMATION AND COMMUNICATION TECHNOLOGIES FOR HUMAN RIGHTS (World Bank, 2012).

<sup>74</sup> ICCPR, *supra* note 2, art. 19.

<sup>75</sup> Comm'n on Hum. Rts., Summ. Record, 6th Sess., 160th mtg., at 34-35, U.N. Doc. E/CN.4/SR.160 (Apr. 27, 1950) [hereinafter "Summary Record No. 160"]; see also BLANCHARD, *supra* note 52, at 181 (noting a statement of Erwin D. Canham, delegate of the United States to the Conference on Freedom of Information and the Press, that freedom of expression "is not a possession of the press, it is not a right of newspapers, it is a right of the people").

<sup>76</sup> Third Comm. of the General Assembly Summ. Record, 16th Sess., 1073d mtg., Oct. 13, 1961, ¶ 13, U.N. Doc. E/C.3/SR.1073. Similarly, when negotiating the contemporaneous Draft Convention on Freedom of Information, the Albanian representative argued that the rights in that convention should be guaranteed to "legitimate news personnel."



*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

Article 19(2) was explicitly grounded in a commitment to the democratization of expression and information, a democratization now enabled by new technologies more fully than ever before.

Second, Article 19(2) explicitly extends protection to all information and ideas, regardless of their perceived value, creativity, or impact. This is evident from the use of the phrase “of all kinds” and is confirmed by the drafting history. During drafting, the delegates were careful to adopt the broadest possible formulation of the subject matter covered by the article. France sought to clarify the types of information that would be included within the ambit of Article 19(2), but proposals for specific enumerations of subject matter were rejected in favor of a catch all provision, “of all kinds.”<sup>77</sup> As Professor Nowak has explained, “Therefore, there can be no doubt that every communicable type of subjective idea and opinion, of value-neutral news and information, of commercial advertising, art works, political commentary regardless of how critical, pornography, etc., is protected by Article 19(2), subject to the permissible limitations in para. 3.”<sup>78</sup> It is the broadly egalitarian nature and openness of new technologies such as the Internet that enable the full realization of the scope of protection intended by Article 19(2).

Third, some of the worst examples of harmful online conduct are not a result of the technology itself but rather the laws and policies that regulate it. The decision to shield intermediaries from liability for comments posted on their sites,<sup>79</sup> for example, has played an important role in the emergence of sites like Juicy Campus, one of several well-known hosts of abusive and harmful comments.<sup>80</sup> Freedom from liability protected the sites from liability for the comments they hosted and anonymity protected the individual posters.

Even at the time of the drafting of the ICCPR, technology and the connection it enabled was seen as posing both great risks and great opportunities not only for individual rights but also international peace and security more broadly. The drafters did not take a position on how to manage that balance but rather created a framework that required the balancing to occur. The ICCPR protects expression and information as well as the technologies of connection, but also requires states to prohibit “advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.”<sup>81</sup> The emergence of new technologies does not change this basic approach. If anything, the potentially greater harms associated with new technologies require states to develop new strategies for achieving this balance; they do not so fundamentally upset this balance that the framework no longer applies.

---

The representative of the United Kingdom objected, arguing that “the principles laid down related to basic human rights to which all persons were entitled.” U.N. Secretary General, *Provisions Concerning Freedom of Information in the Draft Covenant on Human Rights*, p. 15, Commission on Human Rights, 6th Sess., U.N. Doc. E/CN.4/Sub.1/106, Mar. 6, 1950.

<sup>77</sup> Summary Record No. 165, *supra* note 56, ¶¶ 35, 37.

<sup>78</sup> NOWAK, *supra* note 6, at 341; *see also* SARAH JOSEPH ET AL., *THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS: CASES, MATERIALS, AND COMMENTARY* 519 (2d ed. 2005) (discussing a Canadian case, *Ballantyne v. Canada*, in which the court found Article 19(2) applied to commercial speech).

<sup>79</sup> Section 230 of the Communications Decency Act states: “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” 47 U.S.C. § 230(c)(1).

<sup>80</sup> Daniel J. Solove, *Speech, Privacy, and Reputation on the Internet*, in *THE OFFENSIVE INTERNET: PRIVACY, SPEECH, AND REPUTATION* 15, 23-24 (Saul Levmore et al. eds., 2012).

<sup>81</sup> ICCPR, *supra* note 2, art. 20(2).

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

#### D. The Importance of Means

Article 19(2) protects “media,” which includes technologies of connection such as the Internet. To some extent, perhaps, this might be the end of the discussion. The law is the law, and it is important to know what the law is for its own sake. Skeptics, however, might well argue that this law is misguided. We should not protect technology because technology is a means, not an end. Vince Cerf, for example, has emphasized that the Internet is only a means to an end, and protecting it as an end in and of itself would skew our priorities.<sup>82</sup> After all, human rights should protect humans, not technology. Moreover, protecting technology in this way seems unnecessary. Given its role in ensuring the fulfillment of human rights, there is likely more than sufficient protection for technology in other provisions of human rights treaties, including but not limited to the rights to freedom of expression as well as economic, social and cultural rights.

There are several reasons why Article 19(2)’s protection of the technologies of connection is far more than a matter of semantics. First, protecting technology is important from a legal perspective. Because of the unique and interdependent relationship between expression and means, protecting expression necessarily requires protecting the technologies of connection. Unless we are standing right next to our audience (and sometimes even then, if we need a bullhorn to be heard), limits imposed on the technologies of connection necessarily limit our ability to seek, receive and impart information. In interpreting the similarly worded Article 10 of the European Convention on Human Rights, for example, the European Court of Human Rights (ECtHR) noted that “Article 10 applies not only to the content of information but also to the means of transmission or reception since any restriction imposed on the means necessarily interferes with the right to receive and impart information.”<sup>83</sup> Based on this relationship, the ECtHR found in that case that the state could not prevent a company from receiving television programs through a dish aerial.<sup>84</sup> Without a medium, there would be no expression. Thus, in many ways, the relationship between means and content is not only interdependent but indivisible. Although the ability to express oneself is of course also valuable in and of itself, the rights to share information and expression have meaning largely in terms of the interactions they enable between individuals.<sup>85</sup> Without an audience, there would be no expression.<sup>86</sup>

Second, protecting the technologies of connection fills an important gap in human rights law. There are many decisions about technology that have important consequences for human rights but which do not themselves directly violate international human rights law. These decisions are those that affect the costs for states in violating human rights—decisions which make it easier or

---

<sup>82</sup> Cerf, *supra* note 4.

<sup>83</sup> *Autronic AG v. Switzerland*, Ser. A, No. 178, App. No. 12726/87, (1990) E.H.R.R. 485, 499 (1990).

<sup>84</sup> *Id.*

<sup>85</sup> John Perry Barlow has argued that information is entirely relational: “The value of what is sent depends entirely on the extent to which each individual receiver has the receptors . . . shared terminology, attention, interest, language, paradigm . . . necessary to render what is received meaningful.” John Perry Barlow, *Selling Wine Without Bottles on the Global Net*, THE ECONOMY OF IDEAS, <https://homes.eff.org/~barlow/EconomyOfIdeas.html>. I agree but would add only that the act of expression, even if never received by an audience, can also have an intrinsic value in and of itself to the person engaging in the expression.

<sup>86</sup> See Michael L. Best, *Can the Internet Be a Human Right?*, 4 HUM. RTS. & HUM. WELFARE 23, 24 (2004) (“Like the tree that falls alone in the forest, if there is nobody to hear me, or nobody to whom I can listen, then my information has no force. Thus there arises a need for access to appropriate information technology if I am to have any hope for securing my right to free expression.”). In other words, Article 19(2) “implies a right to communication instead of merely to speak.” Fred H. Cate, *The First Amendment and the International “Free Flow” of Information*, 30 VA. J. INT’L L. 371, 374 (1990).

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

harder to violate human rights law. Protecting the technologies of expression under human rights law allows us to challenge such decisions directly rather than in terms of their potential outcome.

Understanding how technology can affect state incentives to comply with human rights law requires a return to one of the first principles of cyberspace—that technology can regulate behavior. Lawrence Lessig, in his well-known book *CODE: AND OTHER LAWS OF CYBERSPACE*, explained that software code is a regulatory modality. Code, he noted, is a form of architecture that, along with law, markets and social norms, can constrain individual behavior, thus functioning as a kind of “law.”<sup>87</sup> Further, code is a regulatory modality for states as well as individuals. Code regulates the behavior of states by making it more or less costly to undertake particular actions. By making it easier (i.e., less costly) for a government to engage in a particular kind of regulation, technology increases the likelihood that such regulation will occur. In this way, “Seemingly narrow technical choices can have broad and lasting impacts on public policy and individual rights.”<sup>88</sup>

In many instances, choices about technology design or code can affect state incentives to violate human rights without directly constituting a violation themselves. Take, for example, the introduction of the new Internet Protocol (IP) addressing system, called IPv6. An IP address is a numerical label assigned to each device connected to the Internet that helps data find its destination online.<sup>89</sup> Under the prior system of addressing, called IPv4, there were not enough unique IP addresses for every device. As a result, devices on local networks would often share IP addresses, making it more difficult to connect individual identities to online activity. Under the new addressing system, IPv6, there are enough unique numbers for every device, which will make it easier for governments and private companies to track online activity.<sup>90</sup> As Professor Derek Bambauer notes, “China’s push to deploy IPv6 is the country’s desire to increase attribution and accountability online. With a sufficient number of IP addresses, China could allocate a single permanent address to each Internet-connected device, and seek to trace data to that source.”<sup>91</sup> An early proposal in the development of IPv6 would have generated IP addresses by using numbers associated with the user’s network interface card, which would have substantially facilitated the ability of governments to connect online activity with real world people.<sup>92</sup> Using a fixed identifier, even if not connected to one’s personal identity, would have made surveillance even easier and was particularly a problem for mobile phones, which had historically been assigned a new IP address with every connection.<sup>93</sup> Concerns about the impact of these changes on privacy, however, led developers to reject the proposal to generate numbers connected to particular hardware and to introduce measures designed to provide additional privacy protection.<sup>94</sup>

Other examples of how decisions about technology affect human rights without directly violating it abound: Publicly funded municipal wireless systems can be set up to track user activity,

---

<sup>87</sup> LAWRENCE LESSIG, *CODE: AND OTHER LAWS OF CYBERSPACE* 6 (1st ed. 2000); *see also* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 507 (1999).

<sup>88</sup> John B. Morris Jr., *Injecting the Public Interest into Internet Standards*, in *OPENING STANDARDS: THE GLOBAL POLITICS OF INTEROPERABILITY* 3, 3 (Laura DeNardis ed. 2011).

<sup>89</sup> *See* Laura DeNardis, *The Global Politics of Interoperability*, in *ACCESS TO KNOWLEDGE IN THE AGE OF INTELLECTUAL PROPERTY* 497, 500-01 (Gaëlle Krikorian & Amy Kapczynski eds. 2010) (“Every device exchanging information over the Internet possesses a unique number (an IP address) identifying its virtual location, somewhat like a unique postal address identifying a home’s unique physical location.”).

<sup>90</sup> *See* Morris, *supra* note 88, at 3.

<sup>91</sup> Derek Bambauer, *Conundrum*, 96 MINN. L.R. 585, 601 (2011).

<sup>92</sup> LAURA DENARDIS, *PROTOCOL POLITICS: THE GLOBALIZATION OF INTERNET GOVERNANCE* 77-84 (2009).

<sup>93</sup> *Id.* at 81.

<sup>94</sup> *Id.* at 87-88.

*forthcoming 54 Harv. Int'l L.J.* \_\_ (2013)  
Please contact author for an updated version before quoting or citing.

making it easier for the government to engage in monitoring and surveillance, with a disproportionate impact on the economically disadvantaged who are unable to purchase access on more secure networks.<sup>95</sup> Mobile phones can be programmed to automatically capture information about the location of images taken using the camera in the phone.<sup>96</sup> Changes in Facebook's default privacy settings can automatically reveal vital and sensitive information about our health and political activities.<sup>97</sup> Internet transmission protocols can enable instantaneous and invisible censorship of material as it travels from one point to another.<sup>98</sup> Even the architecture of the system itself can have an impact on the behavior of states. As Professors Jyh-An Lee and Ching-Yi Liu note, it is more difficult for states to control speech in networks that are decentralized and open.<sup>99</sup>

Indeed, countries have realized the potential of software code to facilitate their control of the Internet and, by implication, expression and the exchange of information, and they are actively pursuing the adoption of international standards embedding such standards into law. Among other things, states are seeking revisions to the regulations of the International Telecommunication Union (ITU). The ITU is a U.N. agency that allocates global radio spectrum and satellite orbits and develops technical standards for interoperability.<sup>100</sup> In connection with a world conference planned for December 2012, called the World Conference on Telecommunications (WCIT-12), the ITU has proposed revisions to its regulations (ostensibly binding on member states, though difficult to enforce) that would enable the ITU to take a larger role in Internet governance.<sup>101</sup> The proposed regulations would augment state authority to eliminate anonymity and assert national priorities in cyberspace. Technology has become the new battleground for human rights and civil liberties.

Protecting the technology of expression provides a basis for adopting a form of the precautionary principle when the human rights consequences of a technological decision are not clear. In most instances, when the human rights impact of a technological decision is clear, the protection of technology and expression will be generally coextensive. If a protocol will make it easier to track individuals and their online activity, it poses a risk to freedom of expression and information and can be condemned on that basis. Focusing only on consequences is not enough, however, because we might not be able to ascertain the effect on human rights until it is too late—at which point, it may be too late to undo.<sup>102</sup> For example, the human rights consequences of further

---

<sup>95</sup> Nicole A. Ozer, *Municipal Wireless and Its Impact on Privacy and Free Speech*, 41 U.S.F. L. REV. 635, 654 (2007) (“People who have money can select another internet service provider with more privacy and free speech-friendly provisions, while those who cannot afford to pay money for internet access will be forced to pay for it with their privacy and free speech.”).

<sup>96</sup> Ronald Deibert & Rafal Rohozinski, *Contesting Cyberspace and the Coming Crisis of Authority*, in ACCESS CONTESTED: SECURITY, IDENTITY, AND RESISTANCE IN ASIAN CYBERSPACE 21, 25 (Ronald J. Deibert et al eds. 2011).

<sup>97</sup> See REBECCA MACKINNON, CONSENT OF THE NETWORKED: THE WORLDWIDE STRUGGLE FOR INTERNET FREEDOM 117, 144-48 (2012).

<sup>98</sup> The addressing scheme would have enabled monitoring by incorporating into IP addresses information tied to a user's physical location, such as a number embedded in the user's Ethernet card. The transmission protocol would have allowed intermediaries to modify content while in transit. Both of these proposed standards were eventually modified to reflect public policy concerns. Morris, *supra* note 88, at 5.

<sup>99</sup> Jyh-An Lee & Ching-Yi Liu, *Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China*, 13 MINN. J.L. SCI. & TECH. 125, 143 (2012) (“open architecture represents a constraint on government power”).

<sup>100</sup> *Overview*, ITU, <http://www.itu.int/en/about/Pages/default.aspx> (last visited August 29, 2012).

<sup>101</sup> Ryan, *supra* note 3, at 2. The ITU, which has historically focused its efforts on mediating cross-border conflicts over radio spectrum, has recently professed a desire “to increase the role of the ITU in Internet governance so as to ensure maximum benefits to the global community.” *Id.*

<sup>102</sup> *Cf.* LESSIG, *supra* note 87, at 140 (noting that it may take resources to code in privacy, but adding that it will be “[f]ar cheaper to architect privacy protections in now than retrofit them later”).

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

departures from a principle of net neutrality, the idea that “companies providing Internet service should treat all sources of data equally,”<sup>103</sup> are not certain. Allowing Internet service providers to charge for faster transmission speeds for some packets as opposed to others might affect the ability of individuals to express themselves or distort the availability of information available online, but we have no way of knowing for sure in advance. Article 19(2)’s protection of the technology of connection provides a normative basis for acting in such situations. Although the effect on freedom of expression and information is not clear, the effect on technology is. Protection of the media of connection means that changes in technology should be scrutinized closely and that where human rights consequences are suspected (but not established), decisions should be more rather than less conservative.<sup>104</sup> This does not mean protecting human rights at all costs; a precautionary principle as applied to technology poses a risk of stifling innovation. Measures taken pursuant to such a principle must be proportional to the harm sought to be avoided and take into account the likelihood of harm.<sup>105</sup>

Third, protecting technology is important rhetorically. Article 19(2)’s protection of media, including new technologies such as the Internet, will help orient debates on the human rights consequences of technology. As Martha Minow has explained, “[r]ights—as words and as forms—structure attention . . . .”<sup>106</sup> Minow was describing the way in which rights call attention to those without power, but they can also function to call attention to previously invisible issues. Decisions about technology are notoriously invisible. As James Grimmelman has noted, the accountability of software as a regulatory modality is limited because “[i]t may not occur to those regulated by software to think of the man behind the curtain, to conceive of a restrictive design decision as being a decision at all.”<sup>107</sup> As a result, it becomes much easier for states to legislate in ways that have human rights consequences while hiding their motives behind ostensibly neutral decisions about technology. Human rights organizations need to be present in these discussions—and at meetings such as the December WCIT-12—to articulate the human rights impact of the technological decisions under consideration. Explicit protection for the technology of connection would help raise awareness about the human rights consequences of technology and offer opportunities to bring together human rights advocates and technologists. International human rights law must pay attention to the means as well as the ends. To do otherwise is to cede much of the battle.

## II. APPLYING ARTICLE 19(2)

Given that it includes protection for the Internet and other media, what specific obligations does the media clause of Article 19(2) impose? Although drafted over six decades ago, Article 19(2) offers a robust foundation for responding to some of the most challenging issues we face today in the regulation of expression and information online. This section uses the text and drafting history of the ICCPR to articulate the nature of the obligations Article 19(2) imposes with respect to the

<sup>103</sup> *Net Neutrality*, TIMES TOPICS (last updated Dec. 22, 2010), [http://topics.nytimes.com/topics/reference/timestopics/subjects/n/net\\_neutrality/index.html](http://topics.nytimes.com/topics/reference/timestopics/subjects/n/net_neutrality/index.html).

<sup>104</sup> Markus Wagner has discussed in detail the elements of the precautionary principle and critiques of its application outside the field of environmental law and policy. The principle generally includes “a threat of harm to the environment or human health; uncertainty about the risks of human behavior; and subsequent action to avoid the anticipated harmful effect.” Markus Wagner, *Taking Interdependence Seriously: The Need for a Reassessment of the Precautionary Principle in International Trade Law*, 20 CARDOZO J. INT’L & COMP. L. 713, 725 (2012)

<sup>105</sup> *Id.* at 733.

<sup>106</sup> Martha Minow, *Interpreting Rights: An Essay for Robert Cover*, 96 YALE L.J. 1860, 1880 (1987).

<sup>107</sup> James Grimmelman, Note, *Regulation by Software*, 114 YALE L.J. 1719, 1736 (2005).

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

Internet and other new technologies. Among other things, Article 19(2) guarantees a right to seek information, to access technology, and to remain anonymous online, and it limits states' ability to prevent information and ideas from crossing their borders. It provides support for efforts to increase equality of access online and anonymous speech. It casts doubt on real-name identification, tracking, and gateway filtering. The principles derived from Article 19(2) provide a foundation for an emerging "international law of the Internet" that offers important normative reorientation on individual rights for both domestic and international Internet governance debates.

### A. Access to Technology

Article 19(2) protects "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."<sup>108</sup> Although a restrictive reading of this clause might view it as merely extending protection to all expression and information regardless of channel or form, such a reading would render meaningless the phrase, "of all kinds," which already makes clear that the protection of the article extends to all expression. Moreover, the text and drafting history of the article demonstrate that the media clause protects far more, establishing rights of choice, access, and non-discrimination with respect to the technology of connection.

First, the media clause specifically guarantees the ability to access media "of his choice." This indicates that the article protects not only the act of seeking, receiving and imparting information but also the ability of individuals to seek out, choose, and access particular media. The drafting history of the article confirms this interpretation. During discussions about the article in the Sixth Session of the Commission on Human Rights, France proposed the addition of text designed to protect an individual's ability to choose his or her media.<sup>109</sup> The United Kingdom objected because the phrase "served no purpose since freedom of expression obviously included the choice of means."<sup>110</sup> France argued that the article must include this element in order to make clear that "if a person had a right to freedom of expression, that right could be exercised by whatever means he might choose."<sup>111</sup> The delegates thus agreed that the article must protect the ability to choose a particular media and only disagreed on whether it was necessary to state this obligation explicitly.

A right to choose technology requires the state to foster competition and the development of a vibrant media market that can offer individuals choice with respect to the technologies of connection. The Human Rights Committee, for example, has identified as among state duties under Article 19 the obligation to "to prevent undue media dominance or concentration by privately controlled media groups in monopolistic situations that may be harmful to a diversity of sources and views."<sup>112</sup> Without options to choose from, a right to choose one's media would be meaningless.

---

<sup>108</sup> ICCPR, *supra* note 2, art. 19(2).

<sup>109</sup> France, *Amendment to the New Text of Article 17 Proposed by the United States of America*, U.N. Doc. E/CN.4/438/Rev.1 (Apr. 21, 1950).

<sup>110</sup> Summary Record No. 165, *supra* note 56, ¶ 6.

<sup>111</sup> *Id.* ¶ 7.

<sup>112</sup> General Comment No. 34, *supra* note 1, ¶ 40. Nowak, as well, argues that state parties "are, therefore, subject to the duty to prevent excessive media concentration with positive measures, such as with State funding assistance for the press." NOWAK, *supra* note 6, at 344. The duty to prevent excessive media concentration is about ensuring market diversity, not content diversity. As such, it is distinct from the now-defunct "fairness doctrine" of the U.S. Federal Communications Commission, which required "licensed broadcasters: (1) 'to provide reasonable amount of time for the presentation over their facilities of programs devoted to the discussion and consideration of public issues;' and (2) 'to

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

Such a right may be particularly important in the area of mobile phones. Currently, lack of competition between service providers is one of the main obstacles to ensuring the financial accessibility of this technology of communication.<sup>113</sup> Finally, a right to choose technology would also support greater calls for transparency and accountability on the part of online content and service providers. Choice is most meaningful when consumers are informed about the policies and practices of the servers they are choosing.

Second, the text and structure of the clause itself appear to protect a right of access to technology. Article 19(2) specifies that freedom of expression includes the freedom to seek, receive and impart information “through any other media of his choice.” This is an active right, one that protects the ability to engage in particular communicative activities through a medium, rather than simply protecting the expression itself. Moreover, the word “freedom” can be read as extending to the remainder of the article, including media, thus implying an ability to access a medium if necessary for the fulfillment of the right. Other commentators have similarly read Article 19(2) to require that, “With regard to electronic media, they [states] must above all provide for adequate public access.”<sup>114</sup> The Special Rapporteur Joint Declaration maintains that “States are under a positive obligation to facilitate universal access to the Internet.”<sup>115</sup> A right to access would be particularly important in this context given that limits on the technology of speech necessarily limits speech itself.

Turning to the drafting history to confirm this interpretation, the negotiations provide some (albeit not altogether clear) support for the idea that Article 19(2) provides a right to access technology. The negotiating states considered and rejected a proposal to include in Article 19(2) a provision requiring the elimination of particular kinds of barriers to access,<sup>116</sup> but they only did so because they felt this kind of a provision would be more appropriate for a convention than a covenant.<sup>117</sup> Thus, as an initial matter, rejection of this provision indicates that they understood Article 19(2) to be about protecting access to communication channels, even though they believed specific direction as to the measures required to accomplish this goal should be elsewhere. Further, the negotiating history of one such convention, drafted contemporaneously with the ICCPR, is consistent with this interpretation. Resolutions adopted by the Conference on Freedom of Information, charged with drafting a Draft Convention on Freedom of Information, called for, among other things, sharing of teleprinter lines (Resolution No. 14) as well as cooperation “in the procurement and advancement of the facilities for the transmission and dissemination of

---

encourage and implement the broadcast of all sides of controversial public issues.” Barak Orbach, *On Hubris, Civility, and Incivility*, 54 ARIZONA L.R. 443, 450 (2012).

<sup>113</sup> August 2011 La Rue Report, *supra* note 8, ¶ 65.

<sup>114</sup> NOWAK, *supra* note 6, at 344.

<sup>115</sup> Joint Declaration, *supra* note 17, ¶ 6e. The Declaration notes that states should do this through regulatory mechanisms such as pricing regimes and universal service requirements, provide direct support for access such as through community ICT centers, promote awareness about Internet use, and establish special measures to ensure access to disabled and disadvantaged populations. *Id.*

<sup>116</sup> The Conference Draft of the text for the ICCPR included a provision, “Measures shall be taken to promote the freedom of information through the elimination of political, economic, technical and other obstacles which are likely to hinder the free flow of information.” Conference Draft, *supra* note 43.

<sup>117</sup> Summary Record No. 165, *supra* note 56, ¶¶ 67, 72. The Secretary General, in annotating a draft of the ICCPR for the General Assembly, explained that the delegates rejected this provision “mainly on the grounds that they dealt with temporary situations or technical problems, rather than the right to freedom of expression itself, and should not, therefore be included in a universal instrument of a lasting character.” Annotations, *supra* note 58, ¶ 137; *see also* BOSSUYT, *supra* note 50, at 396-97.

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

information” (Resolution No. 22).<sup>118</sup> Although the Draft Convention on Freedom of Information was never adopted or ratified, this was largely because of Cold War politics,<sup>119</sup> and its text and the recommendations of the Conference still provide support for the idea that states were concerned with access to the actual technology of connection.

The existence of a right to access the technology of connection has significant implications for human rights today. Among other things, it would help address the difficult question of “what should be done about the meager and highly concentrated information flows in the least developed countries.”<sup>120</sup> As Special Rapporteur La Rue has noted, access to the Internet is often financially inaccessible for many given limited competition, scarce bandwidth, and the cost of equipment.<sup>121</sup> A right to access technology would provide a strong rhetorical and legal basis for working toward the elimination of the digital divide, as it exists both between and within particular communities.<sup>122</sup> Among other things, it would require states to invest in the infrastructure needed for connection and establish competition policies that lower prices.

A right to access technology would also require careful scrutiny of international policies that risk of exacerbating the digital divide. For example, a recent proposal by the European Telecommunications Network Operators Association (ETNO) calling for revisions to the ITU’s regulations on international IP interconnection poses significant risks for access in developing countries. Currently, global communication between Internet networks is typically handled through commercial agreements that allow networks to exchange data without costs or accounting, a principle known as “settlement free peering.”<sup>123</sup> The ETNO has proposed the adoption of a “sending party network pays” principle, similar to the principle currently in place for international telephone calls, that would allow local network operators to charge termination fees.<sup>124</sup> On the one hand, it is possible that these fees will result in greater wealth transfers to developing countries, thus facilitating the growth of local infrastructure (assuming the fees would be invested in infrastructure, of course).<sup>125</sup> A principle of “sending party pays” also poses significant risks for human rights, however. Carriers might decide not to serve markets that are not large enough to justify the cost.<sup>126</sup> Termination fees might be set prohibitively high, either in an attempt to generate as much revenue as possible or even to block foreign content.<sup>127</sup> It may also lead to less local caching (or storing) of content so that information must be resent each time it is requested, thus leading to increased fees.<sup>128</sup>

---

<sup>118</sup> *Final Act of the United Nations Conference on Freedom of Information*, Annex C, U.N. Doc. E/CONF.679 (April 22, 1948), reprinted in 1948 Y.B. on Hum. Rts. 496, 504. See also Penney, *supra* note 4, at 27-28 (discussing the importance of promoting freedom and accessibility of information mediums to the negotiating states).

<sup>119</sup> Amsterdam Center for International Law, *The UN and Freedom of Expression and Information: Critical Perspectives—Background Information*, UNIVERSITY OF AMSTERDAM, <http://www.jur.uva.nl/aciluk/object.cfm/2C8143EF-1321-B0BE-686CC7F0A055DDAB> (last visited August 3, 2012).

<sup>120</sup> Marshall Conley & Christina Patterson, *Communication, Human Rights, and Cyberspace*, in HUMAN RIGHTS AND THE INTERNET 211, 211 (Steven Hick et al. eds. 2000).

<sup>121</sup> August 2011 La Rue Report, *supra* note 8, ¶ 65.

<sup>122</sup> The digital divide is not only geographic but can also occur along the lines of race, gender, age, and disability. May 2011 La Rue Report, *supra* note 1, ¶ 61; see also Herman Wasserman, *Connecting African Activism with Global Networks: ICTs and South African Social Movements*, 30 AFRICA DEVELOPMENT 163, 174 (2005).

<sup>123</sup> Center for Democracy and Technology, *supra* note 3, at 3.

<sup>124</sup> *Id.* at 4.

<sup>125</sup> See *id.* at 5 (critiquing the argument that sending party pays will foster development).

<sup>126</sup> *Id.*

<sup>127</sup> *Id.* (“Indeed, high termination fees could be used to actively discourage foreign content providers from serving the local market.”).

<sup>128</sup> *Id.* at 5.



*forthcoming 54 Harv. Int'l L.J.* \_\_ (2013)  
Please contact author for an updated version before quoting or citing.

It might also raise the prices of international exchanges, as the cost of sending information is passed on to consumers, and it could impose a particularly significant burden on small businesses in developing countries.<sup>129</sup>

Article 19(2) also provides a basis for an individual right to access *specific* technologies, although this right may be limited to situations in which no adequate alternative means are available for the individual to achieve his or her communication or expressive goals. In interpreting Article 10 of the European Convention on Human Rights (ECHR), the European analog to Article 19, the European Court of Human Rights (ECtHR) affirmed a right to access a particular technology for exchanging expression and information if no other means exist for doing so. In *Khurshid Mustafa & Tarzibachi v. Sweden*,<sup>130</sup> the ECtHR held that a family had an interest in receiving, via a satellite dish installed on the outside of their apartment building, programs originating from the family's country of origin. According to the court, "[t]he right to receive information basically prohibits a government from restricting a person from receiving information that others wish or may be willing to impart on him or her."<sup>131</sup> Emphasizing that the family had no other way to receive the programs,<sup>132</sup> the court found that landlord's stated concerns that the satellite dish constituted a safety hazard and caused physical and aesthetic damage were not sufficient to justify preventing the family from using the dish to receive these programs.<sup>133</sup> Such a right only exists, however, when the technology in question is the only means available for exercising one's rights. For example, while Twitter is a technology of connection covered by the "media" clause of Article 19(2), this does not mean that individuals can claim a right of access to Twitter per se. Article 19(2) provides a right to access technology necessary to ensure meaningful exercise of one's right to freedom of expression and information; it does not provide a right to any particular technology in that process.

A right to access technologies of connection also entails an obligation of non-discrimination with respect to that access. Articles 2(1) and 26 of the ICCPR establish strong principles of non-discrimination and equality, respectively requiring states to respect and ensure the rights in the covenant without regard to status and to affirmatively protect individuals from status-based discrimination. The obligation of non-discrimination with respect to the technology of connection would require states to ensure equal access to these technologies without distinction based on "race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."<sup>134</sup> It also requires states to protect and foster access to technologies of connection (available and financially accessible infrastructure, hardware, software, and platforms) for vulnerable populations, such as those in rural areas, the poor, or individuals with visual impairments.<sup>135</sup>

The obligation of non-discrimination with respect to the technologies of connection has important implications for the network neutrality debate. At its broadest, network neutrality is a principle of network design that requires Internet service providers "to treat all content, sites, and platforms equally."<sup>136</sup> Practices that deviate from a principle of network neutrality can affect human rights. Some of these practices, such as Internet filtering (which violates a principle of network

<sup>129</sup> *Id.* at 3-4.

<sup>130</sup> *Khurshid Mustafa & Tarzibachi v. Sweden*, (2011) 52 E.H.R.R. 24 (2008).

<sup>131</sup> *Id.* ¶ 41.

<sup>132</sup> *Id.* ¶ 45.

<sup>133</sup> *Id.* ¶ 48; see also Robin Elizabeth Herr, Can Human Rights Law Support Access to Communication Technology?: A Case Study under Article 10 of the Right to Receive Information 14-15 (2011).

<sup>134</sup> ICCPR, *supra* note 2, art. 26.

<sup>135</sup> See Sean Williams, Comment, *Closing in on the Light at WIPO: Movement Towards a Copyright Treaty for Visually Impaired Persons and Intellectual Property Movements*, 33 U. PA. J. INT'L L. 1035 (2012).

<sup>136</sup> Tim Wu, *Network Neutrality*, [http://timwu.org/network\\_neutrality.html](http://timwu.org/network_neutrality.html).

*forthcoming 54 Harv. Int'l L.J.* \_\_ (2013)  
Please contact author for an updated version before quoting or citing.

neutrality by blocking some content and not others), do so quite obviously.<sup>137</sup> Other kinds of deviations are more complicated. For example, attention has been focused recently on proposals that would allow Internet service providers to distinguish between, prioritize, and charge more to transmit certain content.<sup>138</sup> Traditionally, networks have operated on a “best effort” basis, treating all content the same and guaranteeing the arrival of none. With the introduction of “quality of service” capabilities, service providers would provide better performance (e.g., greater bandwidth, less delay, higher reliability) for prioritized traffic.<sup>139</sup> Although the Joint Declaration on Freedom of Expression and the Internet authored by UN, OSCE, OAS, and ACHPR experts in the area of freedom of expression takes a firm stand against any discrimination in the treatment of Internet data and traffic,<sup>140</sup> it does not seem that any and all discrimination would *necessarily* violate human rights. Simply charging more for better or faster service does not violate a principle of non-discrimination; indeed, some argue that introducing quality of service capacity will improve overall performance (and thereby access) by allowing Internet service providers to better allocate resources and manage traffic.<sup>141</sup>

Quality of service proposals do, however, pose human rights risks. First, such proposals provide a mechanism and justification for content surveillance. Quality of service requires network operators to monitor content, thus providing an additional avenue for repressive states to control online expression and information.<sup>142</sup> Second, privileging certain packets of information over others also risks hindering expression and the exchange of information directly, since it “could readily be used to make it harder for individual users to receive information that they want to subscribe to, and easier for them to receive information from sites preferred by the provider.”<sup>143</sup> Third, deviations from a principle of network neutrality could constitute discrimination on the basis of economic status or poverty.<sup>144</sup> Providing quality of service might violate human rights because it could lead to the creation of two tiers of online service, priority and non-priority, distinguished by quality and cost. Extreme disparity in quality between the tiers raises equality concerns; permanently relegating the poor to a low-quality medium of expression might also constitute a deprivation of their ability to meaningfully exercise rights of expression and information. Tiered service might also compound the

---

<sup>137</sup> *Id.*

<sup>138</sup> See, e.g., Chloe Albanesius, *Verizon: FCC Net Neutrality Rules Violate First Amendment*, PC MAG.COM (July 3, 2012, 03:17 p.m.), <http://www.pcmag.com/article2/0,2817,2406672,00.asp> (asking whether Amazon should be able to “pay to have its website load faster than a mom and pop ecommerce site, for example”).

<sup>139</sup> *What is QoS?*, WINDOWS SERVER, [http://technet.microsoft.com/en-us/library/cc757120\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc757120(v=ws.10).aspx)

<sup>140</sup> Joint Declaration, *supra* note 17, ¶ 5a (“There should be no discrimination in the treatment of Internet data and traffic, based on the device, content, author, origin and/or destination of the content, service, or application.”).

<sup>141</sup> *What is QoS?*, *supra* note 139 (“Network administrators can use QoS to manage the priority of applications that rely on UDP, such as multimedia applications, so that they have the required bandwidth even in times of network congestion, but do not overwhelm the network.”).

<sup>142</sup> Center for Democracy and Technology, *supra* note 3, at 8.

<sup>143</sup> YOCHAI BENKLER, *THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM* 147 (2006).

<sup>144</sup> See U.N. Human Rights Comm., 35th Sess., Communication No. 196/1985: France (Gueye v. France), ¶ 9.4, CCPR/C/35/D/196/1985 (Apr. 6, 1989); see also Gillian MacNaughton, *Untangling Equality and Nondiscrimination to Promote the Right to Health Care for All*, 11 HEALTH & HUM. RTS.: AN INT’L J. 47, 49-50 (2009), <http://www.hhrjournal.org/index.php/hhr/article/viewFile/173/271> (noting that there is support for recognizing “poverty” as a status in international law and that the term “property” in the UDHR and the corresponding provisions in the ICCPR and ICESCR refer to “economic status”).

*forthcoming 54 Harv. Int'l L.J.* \_\_ (2013)  
Please contact author for an updated version before quoting or citing.

digital divide if non-priority low-quality service is concentrated in already disadvantaged communities and populations.<sup>145</sup>

Human rights might also lead us to be cautious about allowing internet service providers to discriminate based on the identity of the sender because it could contribute to the development of market monopolies and harm individual choice. Historically, the principle of net neutrality meant that internet service providers treated all packets alike regardless of the identity of sender or receiver.<sup>146</sup> Recently, however, providers have been pushing for an increased ability to price discriminate online, including the ability to charge more for content provided by a competitor.<sup>147</sup> Article 19 guarantees the right to choose a media for expression and information. Some price discrimination and price differentiation likely would not so impinge individual choice as to violate Article 19, and could even have welfare maximizing effects.<sup>148</sup> More extreme price differentiations would raise human rights concerns, especially for poor and vulnerable populations whose choices are already restricted. Further, there are concerns that price discrimination against competitors could decrease market diversity, thus hindering individual choice even further. Companies might also implement price discrimination by creating two tiers of service, premium and non-premium,<sup>149</sup> thus raising similar concerns as quality of service proposals.

Given these human rights risks, Article 19 would provide support for government regulations in the area of net neutrality. In the United States, for example, these arguments could be used to pressure the government to address some of the gaps in the Federal Communication Commission's net neutrality rules, such as the exception for Internet services provided at places of business, which could have a differential impact on the poor, who may be required to access the Internet at places outside of their homes.<sup>150</sup> Deviations from a principle of net neutrality—whether quality of service proposals or price discrimination—might also be rendered compatible with human rights if they ensure a “core minimum” of delivery.<sup>151</sup> As Professor Peter Yu explains, this approach, which is drawn from the jurisprudence of the International Covenant on Economic, Social and Cultural Rights (ICESCR), would require states to provide minimum essential levels of protection and, in areas beyond that core, take steps towards full realization of the right.<sup>152</sup> Adopting such an approach here would guarantee that individuals had sufficient access to interconnection and allow price discrimination in areas beyond. Nonetheless, this approach also raises some concerns. As a matter of jurisprudence, it is not clear we should import a concept developed in response to the specific requirements of the ICESCR to the interpretation of the ICCPR. Further, there is always the risk that minimums might become maximums, with states feeling they have satisfied their

---

<sup>145</sup> See MACKINNON, *supra* note 97, at 122-23.

<sup>146</sup> Nicolas Economides, “Net Neutrality,” *Non-Discrimination and Digital Distribution of Content Through the Internet*, 4 I/S: J. L. & POL'Y FOR INFO. SOC'Y 209, 212 (2008).

<sup>147</sup> *Id.* at 227.

<sup>148</sup> Dennis L. Weisman & Robert B. Kulick, *Price Discrimination, Two-Sided Markets, and Net Neutrality Regulation*, 13 TUL. J. TECH. & INTELL. PROP. 81, 101 (2010) (“In its current form, [the FCC's proposed] nondiscrimination rule would actually reduce society's total economic welfare because the weight of the economic evidence suggests that both differential pricing and price discrimination by broadband providers toward content providers increase both static and dynamic efficiency.”).

<sup>149</sup> Economides, *supra* note 146, at 227.

<sup>150</sup> *Preserving the Open Internet*, 76 Fed. Reg. 59192 (Sept. 23, 2011).

<sup>151</sup> My thanks to Peter Yu for this observation.

<sup>152</sup> Peter K. Yu, *Reconceptualizing Intellectual Property Interests in a Human Rights Framework*, 40 U.C. DAVIS L. REV. 1107-08 (2007).

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
 Please contact author for an updated version before quoting or citing.

obligations completely upon fulfillment of the core minimum.<sup>153</sup> Finally, even with the core minimum approach, it is possible that disparities in the tiers of service might become so great that it constitutes discrimination even if a basic level of connection is ensured.

Moreover, because Article 19(2) protects rights of access and choice with respect to technology, limits on access to and choice of technology must meet the requirements of Article 19(3). Article 19(3) provides that the rights to seek, receive and impart information may be limited, but that these limits “shall only be such as are provide 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.”<sup>154</sup> Interpreting this provision, Special Rapporteur La Rue has explained that any limitations on expressive rights must meet the following criteria of legality, legitimacy, and proportionality:

- (a) It must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency); and
- (b) It must pursue one of the purposes set out in article 19, paragraph 3, of the Covenant, namely (i) to protect the rights and reputations of others, or (ii) to protect national security or of public order, or of public health or morals (principle of legitimacy); and
- (c) It must be proven necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality).<sup>155</sup>

Thus, although there may not be a right to access Twitter per se, a decision to cut off access to Twitter would trigger the requirements of Article 19(3). Rights to access and choose technology would thus require careful scrutiny of Internet restricting policies, including proposals to build an “on/off” switch into the Internet, Egypt’s decision to turn off the Internet in January 2012, and graduated response laws and policies in France and elsewhere.<sup>156</sup>

## **B. Access to Information**

In addition to providing a basis for accessing the technology of connection, Article 19(2) also protects access to information online. Although generally thought of in terms of expression, Article 19(2) is far more robust. The article itself protects not only the ability to seek, receive, and impart ideas—quintessential “expressive” rights—but also information. The importance of a right to access information is confirmed by the drafting history. In fact, what eventually became Article 19 was initially referred to as a “right to information” and was understood as protecting both information and expression.<sup>157</sup> As Penney describes, the delegates negotiating the ICCPR viewed information, expression, and opinion as integrally linked.<sup>158</sup> Although they rejected a proposal to

<sup>153</sup> See Peter K. Yu, *Anticircumvention and Anti-Anticircumvention*, 84 DENV. U. L. REV. 13, 67 (2006).

<sup>154</sup> ICCPR, *supra* note 2, art. 19(3).

<sup>155</sup> May 2011 La Rue Report, *supra* note 1, ¶ 24.

<sup>156</sup> See, e.g., *id.* ¶ 49.

<sup>157</sup> Amsterdam Center for International Law, *supra* note 119, at 1. Given its importance for human rights and human security, the emphasis on access to information can be seen as part of the development of what Professor Ruti Teitel calls “the law of humanity,” a framework that emphasizes human rather than state security. RUTI TEITEL, *HUMANITY’S LAW* 4 (2011).

<sup>158</sup> Penney, *supra* note 4, at 23.

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

frame this as a right to “freedom of information and expression,”<sup>159</sup> the drafters did so only because they worried that such a framing would be too narrow. Several states argued that a right to information was already encompassed within the right to freedom of expression,<sup>160</sup> and that this would be sufficiently explicit through mention of “information and ideas.”<sup>161</sup> Indeed, although perhaps counterintuitive today, some viewed freedom of information as more restrictive than freedom of the press, with the former only referring to news agencies and the latter to the rights of citizens to express themselves.<sup>162</sup> Both the states that opposed characterizing this explicitly as an article about freedom of information and expression (as well as those in favor<sup>163</sup>) believed information was and should be protected and that this article should sweep as broadly as possible.

The right to seek, receive and impart information in Article 19(2) implies positive duties for the state in providing access to information, especially government information. Of course, at the time of the drafting of the ICCPR, the dominant human rights paradigm was largely “negative in orientation; it was concerned mainly with promoting the unrestricted flow of information and ideas internationally and across borders, and limiting state restrictions on media and mediums.”<sup>164</sup> Thus, at a minimum, Article 19(2) would prevent the state from interfering with an individual’s ability to seek out generally accessible information, such as by confiscating a journalist’s film.<sup>165</sup> The text, however, would seem to imply positive duties, as well. A right to seek public information would be meaningless if the government did not allow such information to be released. Further, recent interpretations of Article 19(2) have emphasized the importance ensuring access to information, especially government information. In General Comment No. 34, for example, the Human Rights Committee noted that states should “proactively put in the public domain Government information of public interest. States parties should make every effort to ensure easy, prompt, effective and practical access to information” and should “enact the necessary procedures, whereby one may gain access to information.”<sup>166</sup> Special Rapporteur La Rue has similarly emphasized the importance of

<sup>159</sup> The initial proposal before the Sixth Session of the Human Rights Committee specified “freedom of expression,” but the Chinese delegation proposed amending it to “freedom of information and expression, explaining that “[i]nasmuch as the Commission had been concerned for three years with the freedom of information, mention of it appeared indispensable.” Comm’n on Hum. Rts. Summ. Rec., 6th Sess., ¶ 32, U.N. Doc. E/CN.4/SR.163 (May 2, 1950). This was accepted into the baseline text, *see* U.S. Draft, *supra* note 53, but later removed on a motion by France, *see* Amendment by France, *supra* note 109 (proposal); Comm’n on Hum. Rts. Summ. Rec., 6th Sess., ¶ 18, U.N. Doc. E/CN.4/SR.164 (May 1, 1950) [hereinafter “Summary Record No. 164”] (discussion in Commission).

<sup>160</sup> Summary Record No. 164, *supra* note 159, ¶¶ 5, 9, 16 (India, Greece, France). They also expressed concern that mentioning “information” a second time in the article might limit the sweep of the broader term “expression.” *Id.* ¶¶ 3, 7 (India, Greece).

<sup>161</sup> *Id.* ¶¶ 11, 15 (United Kingdom, Philippines).

<sup>162</sup> BLANCHARD, *supra* note 52, at 158; *see also id.* at 261 (“To some delegates, freedom of expression encompassed the other freedoms [of information and opinion], while freedom of information was a narrower, more passive freedom to receive data.”).

<sup>163</sup> China, for example, supported the amendment on the grounds that the UDHR protected both information and opinions and the ICCPR should not be less restrictive than the UDHR. Summary Record No. 164, *supra* note 159, ¶ 8. Australia supported the amendment because “entire history of the article had been bound up with the concept of freedom of information.” *Id.* ¶ 13. The United States said that it had included “information” to make the article more precise since “reception of information and ideas was the prerequisite to the ability to express them.” *Id.* ¶ 6.

<sup>164</sup> Penney, *supra* note 4, at 41; *see also Z v. Austria*, App. No. 10392/83, 56 DR 13. Professor Nowak also expresses doubt about whether the right to information requires the state to affirmatively provide access to state or private information, noting only that many states have started to impose such obligations as a matter of domestic law. NOWAK, *supra* note 6, at 344.

<sup>165</sup> NOWAK, *supra* note 6, at 343.

<sup>166</sup> General Comment No. 34, *supra* note 1, ¶ 19.

*forthcoming 54 Harv. Int'l L.J.* \_\_ (2013)  
Please contact author for an updated version before quoting or citing.

states making available public information, stating that “[g]overnments should take the necessary legislative and administrative measures to improve access to public information for everyone.”<sup>167</sup> Further, states must develop access to information policies that maximize the accessibility and disclosure of public information.<sup>168</sup>

Under an evolutive approach to interpretation, which recognizes that “some treaties in their nature are designed to allow for a more progressive development or elaboration of the treaty,”<sup>169</sup> these current authoritative interpretations should be entitled to significant weight in light of the importance of access to information in our current information environment. Information today plays an increasingly critical role in ensuring the protection of human rights. For example, information plays an essential role in protecting the right to health; lay and professional health care providers alike require information about medical care in order to provide health services.<sup>170</sup> Dissemination of knowledge related to food prices and markets can help farmers obtain better prices for their crops and thus augment their ability to maintain an adequate standard of living for themselves and their families, protected by Article 11 of the ICESCR.<sup>171</sup> Access to public information also plays a central role in facilitating citizen participation in public affairs and accountable government.<sup>172</sup> Information is also critical in fostering the enforcement of human rights. For example, it provides the basis for “naming and shaming” activities as well as the foundation of grassroots organizing and advocacy.<sup>173</sup>

Access, however, is not enough. States also have to work to promote the information capacities of individuals. Information must be not only available but also adequate, accessible, acceptable, and of sufficient quality. It must be sufficient to meet the individual’s informational needs, affordable, physically available, and available without discrimination.<sup>174</sup> Moreover, it must be of sufficient quality—i.e., it must be relevant and reliable.<sup>175</sup> Although one of the great strengths of new technologies and the social practices developed around them has been their ability to generate,

---

<sup>167</sup> 2010 La Rue Report, *supra* note 8, ¶ 32.

<sup>168</sup> *Id.*

<sup>169</sup> GARDINER, *supra* note 35, at 242. As Pierre-Marie Dupuy explains, an evolutive approach is not about adopting a meaning that was not intended by the authors of the treaty, but rather making sure that “a new reading is undertaken in such a way as to reflect the common desire of the parties as if they had renegotiated the same agreement taking into account the circumstances that have since evolved.” Dupuy, *supra* note 59, at 126.

<sup>170</sup> See generally Molly Land & Neil Pakenham-Walsh, *Access to Health Information Under Human Rights Law* (New York Law School Institute for Information Law and Policy White Paper No. 11/12, #1, 2012); Trudo Lemmens & Candice Telfer, *Access to Information and the Right to Health: The Human Rights Case for Clinical Trials Transparency*, 38 AM. J.L. & MED. 63 (2012).

<sup>171</sup> See LAND ET AL., *supra* note 73. The right to seek information might be viewed as a component of the right to science and culture, which the U.N. Special Rapporteur in the Field of Cultural Rights, Farida Shaheed, has described as deeply connected to the ability of individuals “to conceive of a better future that is not only desirable but attainable.” Special Rapporteur in the Field of Cultural Rights, *Report of the Special Rapporteur in the Field of Cultural Rights, Farida Shaheed*, ¶ 20, U.N. Doc. A/HRC/20/26 (May 14, 2012).

<sup>172</sup> 2010 La Rue Report, *supra* note 8, ¶ 31.

<sup>173</sup> LAND ET AL., *supra* note 73.

<sup>174</sup> As a resource right, information might be analogized to economic, social and cultural rights like the right to water. Simply having access to water is not sufficient. Among other things, to be of sufficient quality, water must not only be safe but also “of an acceptable colour, odour and taste for each personal or domestic use.” Committee on Economic, Social and Cultural Rights, *General Comment No. 15: The Right to Water (Arts. 11 and 12 of the International Covenant on Economic, Social and Cultural Rights)*, ¶ 12(b), U.N. Doc. E/C.12/2002/11 (Jan. 20, 2003).

<sup>175</sup> “In order to make sound decisions . . . , we depend on high-quality information.” Urs Gasser, *Regulating Search Engines: Taking Stock and Looking Ahead*, 8 YALE J. L. & TECH. 201, \_\_ (2006).

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

collect, store and transmit vast quantities of data,<sup>176</sup> this is also a weakness: “The problem is no longer one of finding information; rather, it is one of finding the *right* information.”<sup>177</sup> Further, the costs of managing and applying information may be prohibitively high for all but the largest civil society organizations.<sup>178</sup> To ensure that the right to information is meaningful, states must strengthen the capacity of individuals to use the information effectively. In his August 2011 report, for example, the Special Rapporteur noted “the importance of ensuring that individuals possess the necessary skills to make full use of the Internet, or what is often referred to as ‘digital literacy’.”<sup>179</sup> Even more radically, a right to information may place obligations on the state to begin to establish appropriate knowledge systems in areas such as health.<sup>180</sup>

Article 19(2) also explicitly protects the ability of individuals to “seek” information. This right to seek information is a right “*actively* to seek information, which goes beyond mere passive reception.”<sup>181</sup> This is apparent from the plain meaning of the term itself—defined as, among other things, “to go in search or quest of” or “to try to find or discover by searching or questioning”<sup>182</sup>—and confirmed by the drafting history. The word “seek” appeared early in the negotiations over the draft article on freedom of information and expression for the UDHR<sup>183</sup> and the ICCPR.<sup>184</sup> Noting that the word had been omitted from an later version of the proposed article on freedom of expression for the ICCPR, the U.S. Draft reintroduced the word in order to protect “the important right to seek information, as distinguished from the passive right to receive information.”<sup>185</sup> Despite the concerns of some states that the term “seek” might encourage “unrestrained and often shameless probing into the affairs of others,”<sup>186</sup> the delegates insisted on its inclusion and rejected proposals that would have substituted the less active word “gather” in order to “protect active steps to procure and study information.”<sup>187</sup> “Gather” was viewed as protecting only the ability to

<sup>176</sup> In the human rights context, for example, SMS data collection platforms combined with information collection techniques such as crowdsourcing can produce an unprecedented quantity of information about human rights and humanitarian problems around the world. LAND ET AL., *supra* note 73.

<sup>177</sup> Gavin Clabaugh, Remarks at American Society of International Law Annual Meeting (Apr. 4, 1992), in 86 AM. SOC'Y INT'L L. PROC. 604, 605 (1992); *see also* Lemmens & Telfer, *supra* note 170, at 105 (discussing the importance of reliable information). It is for this reason that tools such as search engines that help us find information that is relevant plays a crucial role in fulfilling our information needs. James Grimmelmann, *The Structure of Search Engine Law*, 93 IOWA L. REV. 1, 3 (2007) (“Search engines are the new linchpins of the Internet.”).

<sup>178</sup> Tom McClean, Not with a Bang but a Whimper: The Politics of Accountability and Open Data in the UK, at 11 (Aug. 5, 2011), available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1899790](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1899790); *see also* Edward F. Halpin & Steven Hick, *Information: An Essential Tool for Human Rights Work*, in HUMAN RIGHTS AND THE INTERNET 238, 241-42 (Steven Hick et al. eds. 2000).

<sup>179</sup> August 2011 La Rue Report, *supra* note 8, ¶ 45; *see also* Lea Bishop Shaver, *Defining and Measuring A2K: A Blueprint for an Index of Access to Knowledge*, 4 I/S: J. L. & POL. INFO. SOCIETY 1 (2008) (developing metrics for measuring access to knowledge and including among those education for information literacy).

<sup>180</sup> Lemmens & Telfer, *supra* note 170, at 100.

<sup>181</sup> NOWAK, *supra* note 6, at 343.

<sup>182</sup> *Seek*, DICTIONARY.COM, <http://dictionary.reference.com/browse/seek?s=t&ld=1089>.

<sup>183</sup> Article 21 of the Drafting Committee Draft read: “Every one is free to hold or impart his opinion, or to receive and seek information and the opinion of others from sources wherever situated.” Drafting Committee Draft, *supra* note 39.

<sup>184</sup> Conference Draft, *supra* note 43.

<sup>185</sup> Comm'n on Hum. Rts. Summ. Rec., 6th Sess., ¶ 6, U.N. Doc. E/CN.4/SR.162 (April 28, 1950).

<sup>186</sup> Rep. of 3d Comm., ¶ 22, U.N. Doc. A/5000 (Dec. 5, 1961) [hereinafter “Report of the Third Committee”]; *see also* BOSSUYT, *supra* note 50, at 384; NOWAK, *supra* note 6, at 343. Summaries of the discussions in the Third Committee are available at U.N. Doc. A/C.3/SR.1070-1076, which comprise the summary records of the 1070th to the 1076th meetings of the Third Committee.

<sup>187</sup> NOWAK, *supra* note 6, at 343.

*forthcoming 54 Harv. Int'l L.J.* \_\_ (2013)  
Please contact author for an updated version before quoting or citing.

“passively accept[] news provided by Governments or news agencies.”<sup>188</sup> Any restrictions on this active right to seek information must comply with the limitations of Article 19(3).

The right to seek information, particularly across borders, would provide support for state and private efforts to design and disseminate circumvention technologies—helping to implement, in essence, a human right to circumvent.<sup>189</sup> Of course, such efforts should not become so focused on technology that they ignore the importance of the capacities and freedom of those who use these technologies.<sup>190</sup> Further, the right to seek information may also have implications for debates about providing individuals with information collected about themselves. Certainly, with respect to other people’s personal data, the right to seek information must be balanced against the obligation to protect privacy. Typically, this is accomplished through application of the limiting clause of Article 19(3), which allows limitations on the rights protected in Article 19(2), such as the right to seek information, in order to protect “the rights or reputations of others.”<sup>191</sup> No such limitations can be placed on the right to seek information about oneself, since information is not in that instance being disclosed. The right to seek information in Article 19(2) might support laws that provide individuals with the ability to seek information about themselves,<sup>192</sup> initiatives to provide “direct to consumer” genetic testing,<sup>193</sup> and proposals for regulations giving individuals the ability to access and correct personal and financial data collected about them.<sup>194</sup> (Further, the right to a media of one’s choice would also support proposals for this data to be portable so that consumers have the ability to move their own information from one platform to another.<sup>195</sup>)

Article 19(2) also protects the right to “receive” information. Although implicitly a part of the process of communication, the rights of readers or others receiving expression or information have typically received less attention in the jurisprudence of free expression.<sup>196</sup> Article 19(2) explicitly calls out for protection the rights of individuals to receive information and expression from others, thus guarding not only the quintessential expressive activity of speaking “but also the information-gathering activities that precede speech.”<sup>197</sup> The protection of the “receipt” of expression and

<sup>188</sup> Report of the Third Committee, *supra* note 186, ¶ 22; *see also* BOSSUYT, *supra* note 50, at 384.

<sup>189</sup> *See* Peter K. Yu, *Region Codes and the Territorial Mess*, 30 CARDOZO ARTS & ENT. L.J. 187 (2012) (discussing a human-rights based right to circumvent).

<sup>190</sup> Clay Shirky, *The Political Power of Social Media*, 90 FOREIGN AFF. 28, 40 (2011).

<sup>191</sup> The limitation in question must also meet the requirements of legality and proportionality. *See* May 2011 La Rue Report, *supra* note 1, ¶ 24.

<sup>192</sup> *See, e.g.*, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, 1995 O.J. (L 281/31), arts. 10, 12; Richard H. Thaler, *Show Us the Data. (It’s Ours, After All.)*, N.Y. TIMES (Apr. 23, 2011) (discussing an effort under way in Britain called “mydata,” designed to provide people with information about themselves in a computer friendly way); Kevin J. O’Brien, *Facebook Offers More Disclosure to Users*, N.Y. TIMES (Apr. 12, 2012).

<sup>193</sup> Caroline Wright et al., *People Have a Right to Access Their Own Genetic Information*, GENOMES UNZIPPED (Nov. 3, 2011), <http://www.genomesunzipped.org/2011/03/people-have-a-right-to-access-their-own-genetic-information.php>.

<sup>194</sup> *See* FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 64-68 (March 2012); *see also* Martin Merzer, *FTC Privacy Report Backs More Credit Data Access for Consumers*, FOX BUSINESS (Mar. 30, 2012), <http://www.foxbusiness.com/personal-finance/2012/03/28/ftc-privacy-report-backs-more-credit-data-access-for-consumers/>.

<sup>195</sup> Although such a data portability right would need to be carefully crafted. Peter Swire and Yianni Lagos have critiqued the data portability provisions in the EU Data Protection Regulation as reducing consumer welfare and posing significant data security risks. Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, \_\_ MARYLAND L.R. \_\_, \_\_ (2013) (forthcoming), <http://ssrn.com/abstract=2159157>.

<sup>196</sup> *See* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at “Copyright Management” in Cyberspace*, 28 CONN. L. REV. 981, 1003 (1996).

<sup>197</sup> *Id.* at 1010.



*forthcoming 54 Harv. Int'l L.J.* \_\_ (2013)

*Please contact author for an updated version before quoting or citing.*

information in the ICCPR, drafted in the late 1940s and early 1950s, is not surprising in light of developing Cold War politics. As Margaret Blanchard notes, “[d]uring the years under consideration, freedom of listen meant freedom of people living behind the iron curtain to listen to Voice of America programming.”<sup>198</sup> Applying the limitations principles of Article 19(3) to the right to receive information indicates that this right could be restricted only in the most limited of circumstances. Under Article 19(3), states must pursue a legitimate purpose in order to restrict the rights guaranteed under Article 19(2).<sup>199</sup> Except where disclosure of information violates the privacy of another, the receipt of information alone will rarely cause harm.<sup>200</sup> To the extent states seek to limit the receipt of information, they are doing so in order to prevent the formation of opinions or to deter actions that people may take based on the information. The first is impermissible, since freedom of opinion cannot be limited under any circumstances under Article 19(1), and the second should be regulated separately, as actions and not expressive activity.

Article 19(2) also protects the right to “impart” information. Most obviously, this protects expressive behavior. It also, however, protects the right *not* to impart information. A right to impart information is about autonomy, not just freedom. It grants a right to impart information but also, by necessary implication, also a right not to impart information<sup>201</sup>—in other words, a “right to be forgotten.” One of the most challenging aspects of the online environment is digital permanence. Information that would have once slipped into oblivion now follows us for the remainder of our lives.<sup>202</sup> Granted, this is information largely voluntarily posted and perhaps we should have to suffer the consequences of our actions. On the other hand, when information was posted by someone too young to fully comprehend these consequences, there may be a better case for providing them with a legal option for requesting the removal of this information (often photographs).<sup>203</sup> In the European Union, there have been explicit calls for the creation of such rules.<sup>204</sup> A right to be forgotten might also support the creation of technological tools designed to allow such digital forgetting.<sup>205</sup>

Finally, the right to access information under Article 19(2) extends to information and ideas “of all kinds.”<sup>206</sup> The breadth of the subject matter encompassed by these terms is staggering—indeed, it is difficult to imagine a broader construction. Article 19(2) protects not only political speech and commentary but also the right to seek out, exchange, and impart information of a factual or frivolous nature, both of which have important implications for human rights. As Clay Shirky has explained, in discussing Ethan Zuckerman’s “cute cat theory of digital activism,” frivolous

<sup>198</sup> BLANCHARD, *supra* note 52, at 4.

<sup>199</sup> See ICCPR, *supra* note 2, art. 19(3) (“For the protection of national security or of public order (ordre public), or of public health or morals.”)

<sup>200</sup> See Cohen, *supra* note 196, at 1013 (arguing that “the mere act of reading cannot injure”). Cohen argues that the right to read does not confer a right to information from an unwilling speaker. *Id.* at 1015. In the context of the ICCPR, which explicitly calls out not only the right to receive but also to seek information and expression, this might be viewed as a restriction on the right to seek, not receive, information.

<sup>201</sup> *Wooley v. Maynard*, 430 U.S. 705, 714 (1977) (“We begin with the proposition that the right of freedom of thought protected by the First Amendment against state action includes both the right to speak freely and the right to refrain from speaking at all.”).

<sup>202</sup> Solove, *supra* note 80, at 18 (“People must now live with the digital baggage of their pasts.”).

<sup>203</sup> Anupam Chander, *Youthful Indiscretion in an Internet Age*, in THE OFFENSIVE INTERNET, *supra* note 80, 124, 126-27.

<sup>204</sup> Jeffrey Rosen, *The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google*, 80 FORDHAM L. REV. 1525, 1533-34 (2012); Steven C. Bennett, *The “Right to Be Forgotten”: Reconciling EU and US Perspectives*, 30 BERKELEY J. INT’L L. 161, 162-63 (2012).

<sup>205</sup> Rosen, *supra* note 96, at 1535 (discussing Tiger Text and X-Pire as examples).

<sup>206</sup> ICCPR, *supra* note 2, art. 19(2).

*forthcoming 54 Harv. Int'l L.J.* \_\_ (2013)  
Please contact author for an updated version before quoting or citing.

expression is important for political change because the platforms that we use for social purposes are often also the best platforms for activism because they are difficult to shut down.<sup>207</sup> Social media platforms also take advantage of the existing networks that people use to connect with others in their private lives. Moreover, the free flow of information itself, even if mundane or ordinary, can lead to calls for greater political freedoms.<sup>208</sup>

### C. Anonymity Online

Article 19(2) also protects anonymity online. The ability to remain anonymous is critically important for ensuring freedom of expression. As the Special Rapporteur notes, “throughout history, people’s willingness to engage in debate on controversial subjects in the public sphere has always been linked to possibilities for doing so anonymously.”<sup>209</sup> Anonymity allows people to give voice to things they might not otherwise express for fear of retribution and thereby helps to mitigate the possible chilling effect of public and private surveillance.

The Internet is both a protector of and a threat to anonymous speech. It is a protector of anonymous speech because technology mediates between speech and identity. As the now-famous New Yorker cartoon proclaimed, “On the Internet, nobody knows you are a dog.”<sup>210</sup> At the same time, the Internet is also one of the greatest threats to anonymity. Private companies interested in understanding their consumers’ behavior or enforcing copyrights are requiring users to identify themselves or developing other tracking mechanisms.<sup>211</sup> Even when names are not required, the sheer volume of information collected about each of us, largely by private companies, threatens to reveal our identities to anyone diligent enough to put together the pieces.<sup>212</sup> Governments, as well, are regulating anonymity through chokepoint regulation, identification requirements, and data retention regulations.<sup>213</sup> Indeed, the proposed revisions to the ITU’s regulation, which would set Internet standards for governments around the world, are rife with “repeated references to the need for users to have a recognized identity.”<sup>214</sup> The convergence of public and private interests in identification and increasing efforts to standardize identification technologies does not bode well for anonymous speech on the Internet.

---

<sup>207</sup> Shirky, *supra* note 190, at 37; *see also* Ethan Zuckerman, *The Cute Cat Theory Talk at ETech*, MY HEART’S IN ACCRA (Mar. 8, 2008, 11:29 AM), <http://www.ethanzuckerman.com/blog/2008/03/08/the-cute-cat-theory-talk-at-etech/>.

<sup>208</sup> Peter K. Yu, *Six Secret (and Now Open) Fears of ACTA*, 64 SMU L. REV. 975, 1051-52 (2011) (“While many entertainment products are uncontroversial, highly commercial, and seemingly frivolous, they may create unintended spillover effects in promoting democratic transition in repressive countries.”).

<sup>209</sup> May 2011 La Rue Report, *supra* note 1, ¶ 53; *see also* Global Internet Liberty Campaign, *supra* note 71, at 30 (“Central to free expression and the protection of privacy is the right to express political beliefs without fear of retribution and to control the disclosure of personal identity. Protecting the right of anonymity is therefore an essential goal for the protection of personal freedoms in an online world.”).

<sup>210</sup> Peter Steiner, *On the Internet, Nobody Knows You’re a Dog*, THE NEW YORKER (July 5, 1993), at 61 (cartoon), *available at* <http://www.unc.edu/depts/jomc/academics/dri/idog.html>.

<sup>211</sup> [MF cite]

<sup>212</sup> When AOL released a batch of search queries from its users, for example, reporters were able to use these search queries to identify individual users. Grimmelmann, *supra* note 177, at 18.

<sup>213</sup> [MF cite]; *see also* May 2011 La Rue Report, *supra* note 1, ¶ 55.

<sup>214</sup> *See* Dwayne Winseck, *The ITU and the Real Threats to the Internet, Part IV: the Triumph of State Security and Proposed Changes to the ITRs*, MEDIAMORPHIS (June 19, 2012), <https://dwmw.wordpress.com/2012/06/19/the-itu-and-the-real-threats-to-the-internet-part-iv-the-triumph-of-state-security-and-proposed-changes-to-the-itrs/>.

*forthcoming 54 Harv. Int'l L.J.* \_\_ (2013)  
Please contact author for an updated version before quoting or citing.

Although also protected by the right to privacy under Article 17 of the ICCPR,<sup>215</sup> the ability to remain anonymous in sending, receiving and imparting information and ideas played an important role in the drafting history of the Article 19. During the negotiations, Brazil proposed to amend the article to provide that “[a]nonymity is not permitted.”<sup>216</sup> Although proposed to protect the rights of others, this amendment was opposed on the grounds that “anonymity might at times be necessary to protect the author.”<sup>217</sup> In rejecting the Brazilian amendment, the negotiating parties refrained from taking a position on anonymity: Article 19(2) neither explicitly prohibits nor explicitly protects anonymity. The result is, in essence, a decision to treat anonymity just like any other aspect of the freedom of information and expression. States are free to impose limits on anonymity—and indeed, should do so if necessary to protect the rights and reputations of others—but if those limits affect freedom of expression and information (as they almost inevitably do), they must meet the legality, legitimacy, and proportionality requirements of Article 19(3).<sup>218</sup>

Although this compromise has largely been adequate for balancing the interests at stake in regulating anonymity, it no longer works today. Government limits on anonymity typically occur after the fact of speech. One may always forfeit the ability to remain anonymous by committing crimes, harming others, or otherwise violating the law, for example.<sup>219</sup> Even where states restrain anonymity in advance—such as in Brazil, which prohibits anonymity by law<sup>220</sup>—such restraints are difficult to enforce. Today, however, technology makes it possible to eliminate anonymity absolutely, invisibly, and with a high level of enforceability.<sup>221</sup> Requirements that individuals use their names or identification numbers to go online can be applied instantly to everyone, without exception.<sup>222</sup> Of course, such requirements can be circumvented (as is demonstrated by emergence of a booming black market for identification numbers in South Korea after its experiment with real-name identification),<sup>223</sup> but circumvention is costly. And circumvention can only occur if the user knows their anonymity is being eroded; in many instances, companies track our online consumer behavior without our knowledge or consent. In this new online context, the balance intended by the drafters in Article 19(2) by their silence on anonymity is no longer adequate to protect anonymity and avoid chilling speech and information exchange.

---

<sup>215</sup> ICCPR, *supra* note 2, art. 17.

<sup>216</sup> Report of the Third Committee, *supra* note 186, ¶ 8.

<sup>217</sup> *Id.* ¶ 21; see also BOSSUYT, *supra* note 50, at 379.

<sup>218</sup> See Karl Josef Partsch, *Freedom of Conscience and Expression, and Political Freedoms*, in *THE INTERNATIONAL BILL OF RIGHTS: THE COVENANT ON CIVIL AND POLITICAL RIGHTS* 209, 219 (Louis Henkin ed. 1981). Indeed, in light of the drafting history, Nowak argues that “the anonymous publication of an opinion or information is protected by Article 19(2).” NOWAK, *supra* note 6, at 341.

<sup>219</sup> See Chander, *supra* note 203, at 132 (noting that a federal judge issued subpoenas in the case involving the website Auto Admit, ordering the site to identify the individuals who had posted defamatory and abusive material on the site).

<sup>220</sup> CONSTITUIÇÃO FEDERAL, art. 5, § 4 (Braz.), <http://pdba.georgetown.edu/Constitutions/Brazil/english96.html> (“the expression of thought is free, and anonymity is forbidden”).

<sup>221</sup> Grimmelmann, *supra* note 107, at 1729-31.

<sup>222</sup> See Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, *Mission to the Republic of Korea*, ¶¶ 49-52, Human Rights Council, U.N. Doc. A/HRC/17/27/Add.2, Mar. 21, 2011 (describing Korea’s real-name identification system and noting “concern[] about the impact of such identification systems to the right to freedom of expression”); see also Pirongrong Ramasoota, *Internet Politics in Thailand after the 2006 Coup: Regulation by Code in a Contested Ideological Terrain*, in *ACCESS CONTESTED*, *supra* note 96, at 21, 98 (describing identification requirements in Thailand).

<sup>223</sup> [MF cite]; see also Choe Sang-Hun, *South Korean Court Rejects Online Name Verification Law*, N.Y. TIMES, Aug. 23, 2012 (noting the law was overturned).

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

Creating and disseminating technologies of anonymity and data privacy can help restore the balance intended by the drafters of Article 19(2). Technologies of anonymity are the tools that allow Internet users to mask their identity online and protect the security of their communications. TOR, for example, is free software designed to allow users to read, post to and browse the Internet without revealing their real world location.<sup>224</sup> Anonymity technologies are currently under threat. Special Rapporteur La Rue has noted, for example, that steps are “being taken in many countries to reduce the ability of Internet users to protect themselves from arbitrary surveillance, such as limiting use of encryption technologies.”<sup>225</sup> Technologies of anonymity allow individuals to protect their identity and their communications online; indeed, they may be a particularly effective way of augmenting security because their use is in the hands of the speaker, who can best judge the level of security required. Tools for protecting data privacy and limiting data collection online can also help restore balance. Data privacy and anonymity are closely tied issues because data, even absent real-name identification, can be used to identify individual users.<sup>226</sup> Increasing transparency around and strengthening the ability of consumers to make choices about what information is tracked and stored (such as through the efforts of the World Wide Web Consortium to “defin[e] mechanisms for expressing user preferences around Web tracking and for blocking or allowing Web tracking elements”<sup>227</sup>) would help individuals remain anonymous online and protect their freedom of expression and information.<sup>228</sup>

Of course, in this new online environment, there is also increased harm as a result of anonymity. The Internet’s ability to facilitate the formation of groups with others who share our beliefs and interests can be a tremendous asset in organizing and developing new methods of production,<sup>229</sup> but online groups can also become extremely destructive. As Danielle Keats Citron has explained, the Internet can magnify the dangerous features of groups: Group interactions online lead to feelings of closeness and affirm the negative views of their members. Digital mediation—the ability to interact with people virtually instead of in person—makes it easier to dehumanize others. Anonymity plays a key role in facilitating online harms: “Individuals do and say things online that they would never consider doing or saying offline because they do not feel anonymous and do not fear getting caught.”<sup>230</sup> The Internet provides a particularly attractive forum for those who wish to spread damaging messages, not only because of anonymity but also because of greater accessibility of the message.<sup>231</sup> Further, it lacks active speech intermediaries like newspaper editors that might

<sup>224</sup> Tor, *Anonymity Online*, <https://www.torproject.org/>.

<sup>225</sup> May 2011 La Rue Report, *supra* note 1, ¶ 55.

<sup>226</sup> Professor Julie Cohen has argued that privacy statutes do not respond sufficiently to anonymity concerns because they are directed to the disclosure of information, and free speech can be equally chilled by its collection. Cohen, *supra* note 196, at 1032-33. This distinction, while still important with reference to many privacy statutes, is rapidly losing conceptual force given the ease with which data can be hacked and shared.

<sup>227</sup> *Tracking Protection Working Group Charter*, W3C, <http://www.w3.org/2011/tracking-protection/charter> (last visited August 28, 2012); see also Federal Trade Commission, *supra* note 194, at 4-5 (calling for “Do Not Track” button); *Universal Web Tracking Opt Out*, DO NOT TRACK, <http://donottrack.us/> (last visited August 28, 2012).

<sup>228</sup> See Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Ambeyi Ligabo, *Implementation of General Assembly Resolution 60/251 of March 2006 Entitled “Human Rights Council,”* Jan. 2, 2007, ¶ 41, Human Rights Council, 4th Sess., U.N. Doc. A/HRC/4/27 (condemning user tracking and the collection of data about users as restricting the rights to privacy and freedom of expression).

<sup>229</sup> See generally CLAY SHIRKY, *HERE COMES EVERYBODY: THE POWER OF ORGANIZING WITHOUT ORGANIZATIONS* (2009).

<sup>230</sup> Danielle Keats Citron, *Civil Rights in Our Information Age*, in *THE OFFENSIVE INTERNET*, *supra* note 80, at 31, 36-37.

<sup>231</sup> Saul Levmore, *The Internet’s Anonymity Problem*, in *THE OFFENSIVE INTERNET*, *supra* note 80, at 50, 53 (comparing the Internet with a bathroom wall and noting the advantages of the Internet).

*forthcoming 54 Harv. Int'l L.J.* \_\_ (2013)  
Please contact author for an updated version before quoting or citing.

otherwise exercise control over the messages they transmit (whether out of reputational concerns, market pressures, or the threat of legal liability).<sup>232</sup> The result of this “perfect storm” of destructive group dynamics and changes in the technological environment can lead to an especially vicious kind of cyber-harm, frequently targeting women and minorities. Victims are threatened, stalked, and harassed, often suffering significant and enduring emotional and physical trauma.

Although there is an increased need for the protection of anonymity in today’s digital environment, there is also an increased need for governments to protect people from cyber-harms. The decision of governments such as South Korea to impose real-name identification requirements are often directed toward introducing more civility online and mitigating the harms of malicious and false rumors and attacks on reputation.<sup>233</sup> Such wholesale approaches that eliminate anonymity completely do not meet the proportionality requirement of Article 19(3), however. Requiring identification ahead of time eliminates anonymity for both harmful and protected speech alike. It also removes anonymity for the act of seeking information, which (absent intrusion into someone else’s privacy) does not typically cause harm. Governments seeking to regulate anonymity in order to protect others should instead consider more targeted approaches—such as augmenting civil, criminal, administrative and civil rights remedies; or limiting intermediary immunity so that intermediaries have an incentive to control for such behavior.<sup>234</sup> Continued reliance on post-speech limits on anonymity tailored to address the particular harm at issue will help restore the balance intended by Article 19(2).

#### D. Online Borders

In addition to protecting technology, access to information, and anonymity, Article 19(2) is also fundamentally committed to a global Internet. Because of its ability to route around blockage and its end-to-end architecture, the Internet has historically been thought of as a quintessentially “global” medium—one that could not and should not be regulated by territorial sovereigns.<sup>235</sup> Increasingly, however, states are imposing borders online. They are doing so along a spectrum of intensity, with some merely seeking to protect certain national values in online environment, such as prohibitions on gambling or Nazi paraphernalia.<sup>236</sup> States and private actors use a variety of techniques to achieve these goals, ranging from the use of geolocational technologies (which

---

<sup>232</sup> *Id.* at 55. Indeed, at least one delegate appears to have supported anonymous expression assuming such expression would be mediated by professionals. The delegate from Saudi Arabia said he would abstain from voting on the Brazilian amendment on the ground that it would be contrary to established literary traditions and violate the privacy of the author; he observed that “provided that his name was known to the editor or publisher, there seemed to be nothing wrong with the practice.” Third Comm. of the General Assembly Summ. Record, 16th Sess., 1075th mtg., Oct. 17, 1961, ¶ 24, U.N. Doc. E/C.3/SR.1075.

<sup>233</sup> Choe Sang-Hun, *South Korean Court Rejects Online Name Verification Law*, N.Y. TIMES, Aug. 23, 2012 (noting that the real name identification law “was adopted amid widespread concern that Internet users were deluging Web sites with malicious and defamatory comments and false rumors; in a few cases, such statements were blamed in the suicides of celebrities”).

<sup>234</sup> See, e.g., Solove, *supra* note 80, at 25 (proposing a notice and takedown approach for harmful gossip and rumor); Citron, *supra* note 230, at 38-40 (discussing the pros and cons of traditional remedies as well as proposing the use of civil rights remedies).

<sup>235</sup> See, e.g., David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1372 (1996).

<sup>236</sup> See, e.g., Paul Schiff Berman, *The Globalization of Jurisdiction*, 151 U. PENN. L. REV. 311, 389-90 (2002); see generally Anupam Chander, *Trade 2.0*, 34 YALE J. INT’L L. 281 (2009) (discussing what these developments mean for today’s world trading order).

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

pinpoint the geographic location of users) to control of local intermediaries (which control content or the payment instruments used to conduct business online).<sup>237</sup> Other states, however, are taking efforts to nationalize the Internet to the next level. Through techniques such as gateway filtering and intermediary liability, backed up by legal and economic incentives, some states are attempting to create national “intranets” that differ significantly from the Internet available to the rest of the world.<sup>238</sup> States are seeking international support for these efforts through revisions to ITU regulations that would affirm state authority to stop the transmission of information and expression at the border.<sup>239</sup>

To some extent, of course, the creation of borders online is a good thing. People want and need content that is responsive to their particular needs and concerns.<sup>240</sup> In addition, governments want to enforce local laws on the Internet, laws which also reflect the values and priorities of national jurisdictions.<sup>241</sup> On the other hand, there are also problems with borders online: They can violate the civil liberties and human rights of citizens on both sides of the border, prevent people from accessing ideas and expression from other parts of the world and views that differ from their own, and even constitute trade barriers in their own right.<sup>242</sup> Article 19(2) provides an important countervailing force to the rise of borders online by creating an explicit right to seek, receive and impart information *across borders*. Article 19(2) does not prevent states from controlling and even filtering content as it crosses their borders, but it does establish a presumption against such limitations and requires that they meet the legality, legitimacy and proportionality criteria of Article 19(3).

Article 19(2) prevents states from disproportionately burdening information and expression from outside their borders. Article 19(2) guarantees the right to seek, receive, and impart information “regardless of frontiers.”<sup>243</sup> Taken at face value, this phrase might appear to mean that states could not stop foreign content from crossing into their borders. Such an interpretation, however, would be unreasonable, since Article 19 clearly allows states to limit freedoms of expression and information in general and even provides a test for evaluating when such limits are permitted. When the application of ordinary principles of interpretation lead to a result that is absurd or unreasonable, recourse to the drafting history is appropriate.<sup>244</sup> The drafting history indicates that Article 19(2) was intended to create an equivalence between domestic and foreign content. The very first draft of the article on freedom of information and expression for the UDHR

<sup>237</sup> See, e.g., JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 7-13 (2006).

<sup>238</sup> Deibert and Rohozinski call this “cyberspace territorialization.” Deibert & Rohozinski, *supra* note 96, at 36. Cass Sunstein and Robert Putnam have used the term “cyberbalkanization” to refer not to the replication of national borders online but to the fragmentation of online social structures that result from individuals seeking out content that reflects their own world views. See ROBERT D. PUTNAM, BOWLING ALONE 177-78 (2000); CASS R. SUNSTEIN, GOING TO EXTREMES: HOW LIKE MINDS UNITE AND DIVIDE 79 (2009).

<sup>239</sup> See Winseck, *supra* note 214 (arguing that these revisions would “bless[] the efforts of individual countries to build their own closed and controlled national Web 3.0 internet spaces today”).

<sup>240</sup> “[P]eople in different nations tend to read and speak different languages and have different backgrounds, capacities, preferences, desires, and needs. These reflect local differences in history, culture, geography, and wealth. Internet users seek out, and content providers want to provide, congenial content that reflects these differences.” *Id.* at 149.

<sup>241</sup> *Id.* at 150.

<sup>242</sup> See, e.g., Derek Bambauer, John G. Palfrey, Jr., & Jonathan L. Zittrain, *A Starting Point: Legal Implications of Internet Filtering* 8-10 (2004), [http://openet.net/docs/Legal\\_Implications.pdf](http://openet.net/docs/Legal_Implications.pdf).

<sup>243</sup> ICCPR, *supra* note 2, art. 19(2); see also BOSSUYT, *supra* note 50, at 381 (the right to freedom of expression and information is “not to be limited within the confines of any political or territorial entity.”).

<sup>244</sup> VCLT, *supra* note 29, art. 23(b).

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

provided that “[t]here shall be free and equal access to all sources of information both within and beyond the borders of the state.”<sup>245</sup> The Conference Draft replaced this with the phrase “regardless of frontiers.”<sup>246</sup> The original phrasing of this part of Article 19(2)—that access must be “free and equal” for information “both within and beyond” the state’s borders—makes clear that it was intended to require states to treat foreign content like domestic content and to prevent states from disproportionately burdening information and expression from abroad.<sup>247</sup> In addition, in treating foreign and domestic content alike, states must ensure limits on foreign content meet the legality, legitimacy, and proportionality requirements of Article 19(3). In this way, Article 19 is an “international right,” one that guarantees freedom of expression “not only in one’s own country but internationally.”<sup>248</sup>

Although the political climate changed rapidly after the drafting of the UDHR, the text “regardless of frontiers” was included in the ICCPR and remained unchanged during negotiations. Indeed, this phrase was discussed only once. In response to a question about why the UDHR Conference Draft shortened the text to “regardless of frontiers,” Charles Malik, the delegate from Lebanon and a crucial figure in the drafting of the UDHR and ICCPR, explained that this phrase was intended to “enable anyone to seek information outside his own country.”<sup>249</sup> Although initially driven by the United States’ goal of guaranteeing correspondents’ ability “to enter foreign countries, to have access to news sources, and to freely transmit copy from abroad,”<sup>250</sup> this was viewed by others as too much of an intrusion on state sovereignty. In response to these concerns, early drafts of Article 19(2) included a clause specifying that it would not prevent states from stopping the flow of people across its borders.<sup>251</sup> By implication, then, the language “across frontiers” was left to govern (and limit states’ ability to control) the flow of information across borders.

Historical developments later in the drafting of the ICCPR does indicate that some caution is warranted in drawing inferences from the inclusion of this particular phrase, taken from the UDHR, in the ICCPR. The drafting of the UDHR in the late 1940s took place in a particular ideological framework, one that viewed the free flow of information across borders as centrally important to international peace and security. Although the U.S. position was also driven in part by a desire to export the U.S. First Amendment abroad, the United States and others broadly held the view that barriers to the exchange of information across borders had contributed to the recent world war.<sup>252</sup> As the 1950s progressed, this viewpoint met with greater and greater resistance, with both developing and Soviet-bloc states increasingly allied against the “unrestricted” vision of freedom of information espoused by the United States and the United Kingdom. Thus, although the states

---

<sup>245</sup> Secretariat Draft, *supra* note 38; *see also* Humphrey, *supra* note 40, at 183-84.

<sup>246</sup> Conference Draft, *supra* note 43.

<sup>247</sup> The rhetoric that surrounded the drafting of this article—although overblown—indicates the extent to which states felt even this limitation to be a significant restriction on their sovereignty. The delegate from the USSR argued that this language “was too wide in scope and could lead to abuses, for it could protect any act of espionage. No State could allow a foreigner to collect any kind of information within its boundaries without any control. Articles 17 and 18, as now drafted, represented a violation of national sovereignty.” Comm’n on Hum. Rts. Summ. Rec., 3rd Sess., p. 3, U.N. Doc. E/CN.4/SR.64 (June 17, 1948) [hereinafter “Summary Record No. 64”].

<sup>248</sup> Partsch, *supra* note 218, at 217.

<sup>249</sup> Summary Record No. 165, *supra* note 56, ¶ 49.

<sup>250</sup> BLANCHARD, *supra* note 52, at 158-59.

<sup>251</sup> Conference Draft, *supra* note 43.

<sup>252</sup> Cate, *supra* note 86, at 374; *see also* BLANCHARD, *supra* note 52, at 61 (noting that one of the arguments in favor of promoting freedom of expression on the UN’s agenda, advanced by the representative of the Philippines, was that “A free press . . . might be the world’s only chance to save itself from the atom bomb.”).

*forthcoming 54 Harv. Int'l L.J.* \_\_ (2013)  
Please contact author for an updated version before quoting or citing.

stood behind it uniformly during the debates about the UDHR and did not challenge it in negotiating the ICCPR, the phrase reflects a world view that subsequently came under considerable pressure from developing states and the East.<sup>253</sup>

The phrase “regardless of frontiers” would prohibit the creation of national cyberzones that differ significantly from the global Internet because such zones constitute a disproportionate burden on foreign information and expression. States are increasingly using a variety of technological, legal and economic techniques aimed at creating national “intranets” that differ significantly from the global Internet. These techniques include filtering and blocking (both automatic filtering at gateway points, discussed below, as well as laws that require intermediaries to control and block specific content); economic policies that support national Internet services providers or which make “domestic content easier and less expensive to access than foreign;”<sup>254</sup> investing in access points that are “tied to special Internet connections, which limit access only to resources found in the national Internet domain;”<sup>255</sup> as well as affirmative propaganda campaigns designed to populate locally available sites with approved information.<sup>256</sup> Collectively, these activities disproportionately burden foreign content and thus violate Article 19(2).

The obligation to avoid disproportionately burdening foreign content would also require careful scrutiny of the practice of gateway filtering. Several countries, including China, employ Internet filtering at the “backbone level,” which is the actual physical infrastructure of cables and routes that connects “the domestic Internet to global networks.”<sup>257</sup> As Professors Lee and Liu explain, “Because online information enters the country through a limited number of connection points, the Chinese government can control the information by controlling these connection points.”<sup>258</sup> At each of these connection points or “gateways,” the government (with the help of the U.S. company Cisco) has installed a router that can drop specified IP addresses.<sup>259</sup> Users who seek to access those IP addresses will simply receive the message that the desired website was not found, a message indicating the network has timed out, or other error code.<sup>260</sup> Collectively, this set of gateway filters has been called the “Great Firewall of China” because of its ability to block undesirable

---

<sup>253</sup> This pressure eventually manifested itself in the late 1950s and 1960s in the push for a “New Information and Communication Order,” headed by the United Nations Educational, Scientific and Cultural Organization (UNESCO). It was UNESCO’s support for this agenda, and the corresponding limitations on the press it advocated, that eventually led the United States to withdraw support from UNESCO. *Id.* at 388-92; *see also* BLANCHARD, *supra* note 52, at 401.

<sup>254</sup> Deibert & Rohozinski, *supra* note 96, at 36.

<sup>255</sup> *Id.* at 27.

<sup>256</sup> *See* Dwayne Winseck, *Big New Global Threat to the Internet or Paper Tiger?: the ITU and Global Internet Regulation, Part I*, MEDIAMORPHIS (June 10, 2012), <http://dwmw.wordpress.com/2012/06/10/big-new-global-threat-to-the-internet-or-paper-tiger-the-itu-and-global-internet-regulation-part-i/> (“In the Web 3.0 model, authoritarian states use filtering and blocking techniques to deny access and (1) establish national laws that put such methods on a firm legal footing, (2) carve out a distinctive national internet-media space dominated by national champions (Baidu, Tencent, Yandex, Vkontakte) instead of Google, Facebook and Apple, within which (3) the state actively uses ‘internet-media-communication’ campaigns (propaganda) to shape the total information environment.”).

<sup>257</sup> Lee & Liu, *supra* note 99, at 133.

<sup>258</sup> *Id.*

<sup>259</sup> GOLDSMITH & WU, *supra* note 237, at 93. An “IP address” is a number assigned to each device on the participating network. Dropping the IP address means blocking, through a variety of means, requests for information from devices with that address. *See* Steven J. Murdoch & Ross Anderson, *Tools and Technology of Internet Filtering*, in ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 57, 59-60 (Ronald Deibert et al. eds. 2008). The result is that websites located on computers with blocked IP addresses will not appear on the user’s computer.

<sup>260</sup> GOLDSMITH & WU, *supra* note 237, at 94.



*forthcoming 54 Harv. Int'l L.J.* \_\_ (2013)  
Please contact author for an updated version before quoting or citing.

content from abroad—just as the Great Wall of China was designed to block foreign invaders.<sup>261</sup> Other states, such as Saudi Arabia, Pakistan and Thailand, have similarly built centralized control points into their Internet infrastructure and used these control points to implement filtering systems at the international-gateway level.<sup>262</sup>

At least with respect to countries that are parties to the ICCPR, such as Pakistan and Thailand,<sup>263</sup> Article 19(2) casts doubt on the practice of gateway filtering. Although the other social and legal mechanisms that countries use to control online content, such as surveillance or licensing, are also highly effective in their own ways,<sup>264</sup> gateway filtering presents particular challenges for free expression. Gateway filtering is more effective and less expensive for governments because it does not rely on compliance by individual ISPs to block content. Absent gateway filters, which operate automatically, governments must turn to ISPs to block prohibited sites, and the resulting filtering may be more variable and less consistently enforced.<sup>265</sup> Australia, for example, which has a more decentralized Internet infrastructure, has not been able to rely on gateway filtering and has found it difficult, as a result, to “deploy[] an effective filtering system.”<sup>266</sup> Further, gateway filtering is also more difficult for users to circumvent.<sup>267</sup> Thus, countries that filter foreign content at deeper levels than domestic content are disproportionately limiting access to information and ideas across borders and triggering the protection of Article 19(2).<sup>268</sup>

### III. IMPLEMENTING ARTICLE 19

This section considers the issue of implementation and non-state actors. Relying on the text and drafting history of Article 19, this section argues that it applies directly to the activities of private actors that substantially burden freedoms of expression and information. Article 19(2) therefore provides a basis for increased transparency and accountability for online intermediaries, including the development of digital due process standards. In addition to bearing direct responsibility for some aspects of freedom of expression and information, this section also argues that technologies companies should be—indeed must be—a central part of an affirmative vision of online freedom. These companies not only determine the development of the technology itself (the code and

---

<sup>261</sup> Lee & Liu, *supra* note 99, at 133. Others include as part of the “Great Firewall” the entire range of techniques that China uses to control online content, including intermediary licensing, surveillance, and punishment. See Milton L. Mueller, *China and Global Internet Governance: A Tiger by the Tail*, in ACCESS CONTESTED, *supra* note 96, at 177, 181.

<sup>262</sup> Lee & Liu, *supra* note 99, at 142; Robert Faris & Nart Villeneuve, *Measuring Global Internet Filtering*, in ACCESS DENIED, *supra* note 259, 1, 14; Ramasoota, *supra* note 222, at 98.

<sup>263</sup> Status of International Covenant on Civil and Political Rights, United Nations Treaty Collection, [http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg\\_no=IV-4&chapter=4&lang=en](http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en). China and Saudi Arabia are not parties to the ICCPR. *Id.*

<sup>264</sup> In addition to gateway and ISP level filtering, states employ a range of second- and third-generation controls, including through laws and regulation that encourage self-censorship and affirmative misinformation and propaganda. See Deibert & Rohozinski, *supra* note 96, at 30-31.

<sup>265</sup> “When filtering is delegated to the ISP level, and hence decentralized, there may be significant differences among ISPs regarding the filtering techniques used and the content that is filtered.” Faris & Villeneuve, *supra* note 262, at 16.

<sup>266</sup> Lee & Liu, *supra* note 99, at 143.

<sup>267</sup> Murdoch & Anderson, *supra* note 259, at 65 (“For countries with tightly controlled Internet connectivity, these measured [such as IP filtering] can also be placed at the international gateway(s), which makes circumvention more difficult and avoids ISPs being required to take any action.”).

<sup>268</sup> Many countries focus their filtering efforts on locally produced content. See Faris & Villeneuve, *supra* note 262, at 21. Article 19(2) also prohibits censorship of local content that does not meet the requirements of Article 19(3), but this does not trigger the phrase “regardless of frontiers.”

*forthcoming 54 Harv. Int'l L.J.* \_\_ (2013)  
Please contact author for an updated version before quoting or citing.

architecture of online expression and information) but often contribute to the development of standards that foster convergence on particular technologies. Technology companies should embed “human rights defaults” into their technology by designing it in ways that make it harder for states to violate international human rights.

### A. Non-State Actors

A central challenge for Internet regulation is the private ownership and regulation of the infrastructure of the Internet. As Special Rapporteur La Rue notes, “the way in which information is transmitted [on the Internet] largely depends on intermediaries, or private corporations which provide services and platforms that facilitate online communication or transactions between third parties, including giving access to, hosting, transmitting, and indexing content.”<sup>269</sup> As these third parties gain ever greater shares of the online market and audience, intermediary choices about what content they will transmit or display increasingly begin to look like a kind of censorship. Rebecca MacKinnon, for example, recounts controversy over Apple’s review process for new applications or “apps” for its iPhone platform. Among other things, Apple refused to carry an app featuring the work of cartoonist Mark Fiore that ridiculed President Obama as well as two apps that respectively “aimed to help ‘cure’ gay men of their homosexuality” and “condemned homosexuality as ‘immoral.’”<sup>270</sup> While the press had historically always played a role as an intermediary in the regulation of speech,<sup>271</sup> that role is filled today by Internet service and content providers and other technology companies. Moreover, the role of these companies has increased exponentially as the opportunities for expression have expanded through the availability of online platforms.

States compound this problem by outsourcing regulation of online content to these intermediaries. Intermediary liability refers to the practice of holding intermediaries such as ISPs “liable for the content disseminated or created by their users.”<sup>272</sup> This practice “severely undermines the enjoyment of the right to freedom of opinion and expression, because it leads to self-protective and over-broad private censorship, often without transparency and the due process of law.”<sup>273</sup> The Chinese government, for example, requires intermediaries to remove prohibited content but refrains from identifying precisely what content is prohibited; this ambiguity leads intermediaries to self-censor and, in many cases, results in over-blocking.<sup>274</sup> Even efforts to protect intermediaries from liability through notice and takedown safe harbors can have the effect of outsourcing responsibility for regulation. Intended to shield intermediaries by providing them with immunity from liability if they comply with certain conditions (such as removing the challenged content), notice and takedown laws can nonetheless lead to overbroad private censorship when intermediaries, under the threat of penalties for failure to respond adequately, “err on the side of safety by overcensoring potentially illegal content.”<sup>275</sup> Such outsourcing of decisions about the regulation of online activity poses

<sup>269</sup> May 2011 La Rue Report, *supra* note 1, ¶ 38.

<sup>270</sup> MACKINNON, *supra* note 97, at 126-27.

<sup>271</sup> BLANCHARD, *supra* note 52, at 28.

<sup>272</sup> May 2011 La Rue Report, *supra* note 1, ¶ 40.

<sup>273</sup> *Id.*; see also *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL*, European Court of Justice, Case No. C-70/10, Nov. 24, 2011 (invalidating injunction requiring ISP filtering in part because “that system might not distinguish adequately between unlawful content and lawful content”).

<sup>274</sup> MACKINNON, *supra* note 97, at 36-40.

<sup>275</sup> May 2011 La Rue Report, *supra* note 1, ¶ 41; see also 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, 687-88 (2006).

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

significant problems from a human rights perspective. There is often no transparency about the decisions reached by these third parties, which compounds efforts to hold them accountable. Intermediaries also lack the expertise, information, and resources to make difficult choices about conflicting values and rights, and as a result are generally “not best placed to make the determination of whether a particular content is illegal, which requires careful balancing of competing interests and consideration of defences.”<sup>276</sup>

Unlike U.S. constitutional law and most of international human rights law, which typically apply only to state action, Article 19(2) imposes obligations directly on third party intermediaries in some instances. Broadly speaking, there are three ways to conceptualize the responsibility of private actors for violations of international human rights law.<sup>277</sup> Most frequently, human rights law assumes these actors do not have any independent duties and turns to governments to protect individuals, through domestic law, from violations of their rights by such parties.<sup>278</sup> The 2008 report of the U.N. Special Representative of the Secretary General on Human Rights and Transnational Corporations and other Business Enterprises, John Ruggie, for example, explains that states have a duty to “take all necessary steps to protect against such abuse, including to prevent, investigate, and punish the abuse, and to provide access to redress.”<sup>279</sup> At times, although less frequently, international law also imposes duties on private actors themselves.<sup>280</sup> Finally, it is also possible to think of human rights obligations as moral or ethical duties, not legal obligations. The Ruggie Report argues, for example, that corporations have the obligation to respect rights, grounding this obligation in “social expectations—as part of what is sometimes called a company’s social license to operate.”<sup>281</sup>

With respect to Internet intermediaries, most of the conversation about human rights has focused on the first and third of these approaches—the obligation of states to protect individuals from violations of their rights by private actors, and the moral or ethical duties of corporations. Proposals for legislation like the Global Online Freedom Act emphasize the responsibility of the U.S. government to control intermediaries and to prevent them from violating human rights.<sup>282</sup> The Global Network Initiative provides, among other things, a framework of best practices and an assessment mechanism for evaluating the human rights performance of companies in the ICT sector.<sup>283</sup> The Berkman Center, the Center for Democracy and Technology, and the non-profit

---

<sup>276</sup> May 2011 La Rue Report, *supra* note 1, ¶ 41.

<sup>277</sup> John H. Knox, *Horizontal Human Rights Law*, 102 AM. J. INT’L L. 1, 1 (2008).

<sup>278</sup> *Id.* (discussing the general obligation of states to “use due diligence to ensure that human rights are protected from private interference”).

<sup>279</sup> Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, *Protect, Respect and Remedy: A Framework for Business and Human Rights*, ¶ 18, U.N. Doc. A/HRC/8/5 (Apr. 7, 2008) [hereinafter “Ruggie Report”].

<sup>280</sup> Knox, *supra* note 277, at 2. In rare cases, human rights law also enforces these duties. *Id.*

<sup>281</sup> Ruggie Report, *supra* note 279, ¶ 54. In some instances, one might also make the argument that when a government delegates responsibility for regulating online content to third parties, “censorship under such pervasive nominally private systems at the behest of the national government is properly chargeable to the state.” Dawn C. Nunziato, *How (Not) to Censor: Procedural First Amendment Values and Internet Censorship Worldwide*, 42 GEO. J. INT’L L. 1123, 1139 (2011).

<sup>282</sup> See Cindy Cohn et al., *Global Online Freedom Act 2012 Is an Important Step Forward*, ELECTRONIC FRONTIER FOUNDATION (Apr. 18, 2012), <https://www.eff.org/deeplinks/2012/04/global-online-freedom-act>.

<sup>283</sup> *About Us*, GLOBAL NETWORK INITIATIVE, <http://www.globalnetworkinitiative.org/about/index.php> (last visited August 10, 2012).

*forthcoming 54 Harv. Int'l L.J.* \_\_ (2013)  
Please contact author for an updated version before quoting or citing.

Business for Social Responsibility have all drafted guiding principles for companies in this area.<sup>284</sup> Others have emphasized the way in which the technology itself and the opportunities it creates can be associated with particular responsibilities. Anupam Chander, for example, has argued that new media companies have special responsibilities, including to distant peoples, because of “the special role of new media in empowering individuals.”<sup>285</sup>

The drafting history of Article 19(2), however, reveals that there is also a basis for applying it *directly* to the conduct of private actors. Article 19(2) provides that “[e]veryone shall have the right to freedom of expression,” but does not specify whether it intends to apply this to public or private actors. In light of this ambiguity, it is appropriate to turn to the drafting history. Throughout the drafting of the ICCPR, there were two competing understandings of the scope of what became Article 19(2): “One was that the article was intended to protect the individual only against governmental interference. The other view was that the article should protect the individual against all kinds of interference.”<sup>286</sup> The United States and the United Kingdom, for example, both supported a draft of the article that would guarantee the “right to freedom of information and expression without governmental interference.”<sup>287</sup> They did not believe there was a significant threat to expression by private actors and were concerned that extending the article to private interference would lead to complications; they also felt that if included, such a provision would require much more detailed treatment.<sup>288</sup>

The delegates, however, explicitly declined to include the phrase “without governmental interference” because they wanted the article to apply to private conduct. A majority of the representatives, led by France, opposed the phrase “without governmental interference,”<sup>289</sup> because “private financial interests and monopoly control of media of information could be as harmful to the free flow of information as governmental interference, and that the latter should therefore not be singled out to the exclusion of the former.”<sup>290</sup> France, Denmark, and Lebanon, in particular, all spoke out about the importance of the threat to expression and information posed by private conduct.<sup>291</sup> Lebanon argued, for example, that “[i]n many countries, private interference from groups of individuals was more to be feared than governmental interference.”<sup>292</sup> Statements of the

---

<sup>284</sup> See Erica Newland et al., *Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users* (Sept. 2011); *Business for Social Responsibility, Applying the UN Guiding Principles on Business and Human Rights to the ICT Industry* (Aug. 2011).

<sup>285</sup> Anupam Chander, *Googling Freedom* 6, 22 (UC Davis Legal Studies Research Paper Series, Research Paper No. 217, 2010).

<sup>286</sup> Annotations, *supra* note 58, ¶ 122; see also BOSSUYT, *supra* note 53, at 379.

<sup>287</sup> U.S. Draft, *supra* note 53.

<sup>288</sup> See, e.g., Summary Record No. 160, *supra* note 75, ¶¶ 27, 36 (statement of U.S. delegate that deleting text “would create complications and give rise to many unpredictable situations” and by UK delegate that proposal would require “fuller treatment”); Summary Record No. 163, *supra* note 53, ¶ 28 (statement of U.S. delegate that “the principal source of interference was censorship enforced by the State”); Summary Record No. 165, *supra* note 56, ¶ 15 (statement of the U.S. delegate admitting that private interference existed but that “it would be difficult to expose or prevent them”); see also, e.g., Summary Record No. 320, *supra* note 55, p. 4 (opposition by United Kingdom in Eighth Session of Commission on Human Rights to include private conduct because it would be “impossible to provide in a single article a code governing conduct in the field of personal relationships”). See generally BLANCHARD, *supra* note 52, at 260 (discussing the US position).

<sup>289</sup> Summary Record No. 165, *supra* note 56, ¶ 17 (adopting French proposal to eliminate the words “governmental interference” from the baseline text).

<sup>290</sup> Annotations, *supra* note 58, ¶ 24; see also BOSSUYT, *supra* note 50, at 385.

<sup>291</sup> Summary Record No. 160, *supra* note 75, ¶¶ 45-46.

<sup>292</sup> Summary Record No. 163, *supra* note 53, ¶ 42.

*forthcoming 54 Harv. Int'l L.J.* \_\_ (2013)  
Please contact author for an updated version before quoting or citing.

representatives involved in negotiation demonstrates that they explicitly understood the removal of the phrase, “government interference,” to extend liability under Article 19(2) to private actors.<sup>293</sup> Subsequent commentators have also concluded that Article 19(2) applies to both public and private conduct.<sup>294</sup>

Article 19(2) not only imposes on governments the obligation to protect the rights of individuals from violations by third parties but also requires private actors to be treated like state actors in some instances. First, Article 19(2), like other human rights provisions, requires the state to act to protect private rights. Indeed, during the drafting history, it was clear this was an important part of what the delegates contemplated.<sup>295</sup> Second, Article 19(2) creates an equivalence between public and private action in some instances. By removing the phrase “without governmental interference,” the delegates ensured that the “right to freedom of expression” was guaranteed against all kinds of interference, both public and private. In this way, Article 19(2) recognizes that with respect to informational and communicative rights, private actors—those who largely own the infrastructure of transmission—can constitute as great of a threat to expression and information as the state.

Article 19(2) creates an equivalence between public and private interference, not public and private activity. Private actors do not trigger the application of Article 19(2) unless and until they interfere with a protected right. In most instances, private activity will not rise to this level. For example, if one hosting service declines to display my content, there are plenty of other services for me to choose from. In that instance, the intermediary has not “interfered” with my right to seek, receive and impart ideas and information. When, however, an intermediary assumes such a dominant market position that its decision not to display my content means that I effectively cannot reach a meaningful audience, that intermediary is “interfering” with my right and must justify its decision according to the three-step test of Article 19(3).<sup>296</sup> This does not mean that private entities triggering this threshold cannot act—it simply means that they cannot act arbitrarily. When a private entity assumes such a dominant position with respect to expressive rights that its conduct threatens to interfere with those rights, it must comply with the legality, legitimacy, and proportionality requirements of Article 19(3). At the very least, this duty would require intermediaries to be more transparent about their activities, “to report regularly and systematically to the public on how content is policed, and under what circumstances it gets removed or blocked and at whose

---

<sup>293</sup> See Third Comm. of the General Assembly Summ. Record, 16th Sess., 1070th mtg., Oct. 11, 1961, ¶ 37, U.N. Doc. E/C.3/SR.1070 (statement by delegate from Iran that in order to cover the range of relevant interference, “[i]t would therefore be necessary either to prohibit all possible forms of interference or to delete the reference to governmental interference”).

<sup>294</sup> See, e.g., NOWAK, *supra* note 6, at 344 (“As with freedom of opinion, freedom of expression is protected not only against interference by public authorities but also against that by private parties.”); Stephanie Farior, *Molding the Matrix: The Historical and Theoretical Foundations of International Law Concerning Hate Speech*, 14 BERKELEY J. INT’L L. 1, 23 (1996).

<sup>295</sup> France argued that the problem of freedom of expression and information simply “could not be dealt with in a general document without considering both of its aspects, namely respect for those freedoms by the State itself and the obligation incumbent upon the State to ensure respect for those freedoms.” Summary Record No. 165, *supra* note 56, ¶ 13.

<sup>296</sup> Similarly, one might argue that although Facebook is entitled to set its own terms of service, it is so widely used as a platform for political activism that its policy of prohibiting pseudonymous pages interferes with the right to freedom of expression and information and must meet the requirements of Article 19(3). See MACKINNON, *supra* note 97, at 151-53 (discussing Facebook’s removal of the “We Are All Khaled Said” page used to facilitate protests against torture in Egypt because it was not registered under a real identity—even though using their real names would have exposed the activists involved to retaliation by the government).

*forthcoming 54 Harv. Int'l L.J.* \_\_ (2013)  
Please contact author for an updated version before quoting or citing.

behest.”<sup>297</sup> Article 19(2) therefore provides a basis for increased transparency and accountability for online intermediaries, including the development of digital due process standards.

Article 19(2) also anticipates and provides a framework for resolving conflicts between the speech rights of individuals and third party intermediaries. Intermediaries have their own expressive interests in choosing what speech and information to convey.<sup>298</sup> Requiring intermediaries whose activities occupy such a dominant place in the market that they are effectively acting like state actors, to justify the choices they make about content is a burden on the intermediary’s own speech. Article 19(3) however, acknowledges and sanctions this additional burden if needed to protect the rights of others. Article 19(3) specifies that “[t]he exercise of the rights provided for in paragraph 2 of this article [namely, freedom of expression and information] carries with it special duties and responsibilities.”<sup>299</sup> Because of this special status, freedom of expression and opinion can be limited in order to protect, among other things, “the rights and reputations of others.”<sup>300</sup> Thus, Article 19(3) recognizes that all those who exercise their own expressive rights under Article 19(2), including speech intermediaries, are subject to duties in the process, and because of those duties, their rights may be limited if necessary to protect the rights of others to express themselves.

The drafting history confirms this interpretation and further clarifies the nature of the duties that the drafters contemplated. During the negotiation of the ICCPR, states on several occasions expressed concern that individuals would exercise their own expressive rights in ways that harmed the rights of others.<sup>301</sup> This was a particular concern in light of the dominance that could be achieved by some voices at the expense of others in situations of media concentration.<sup>302</sup> The language of “duty” was added to make clear that “opinion makers” were obligated “not to abuse their power at the expense of others.”<sup>303</sup> Thus, intermediaries are free to exercise their own rights, but if they interfere with the rights of others in the process and by virtue of their dominance in the market, they can be called on to justify their choices within the framework of Article 19(3).

## B. Human Rights Defaults

Enforcing Article 19 with respect to non-state actors raises all the difficulties of enforcing international law more generally—and then some. The question of how to enforce international law even with respect to states is challenging given that this law “lacks a central governmental authority that has the power to enforce its commands.”<sup>304</sup> In response to critiques that international law

---

<sup>297</sup> MACKINNON, *supra* note 97, at 244.

<sup>298</sup> See Randolph J. May, *Net Neutrality Mandates: Neutering the First Amendment in the Digital Age*, 3 I/S: J. L. & POL’Y FOR INFO. SOC’Y 197, 202 (2007).

<sup>299</sup> ICCPR, *supra* note 2, art. 19(3).

<sup>300</sup> *Id.*

<sup>301</sup> See generally BOSSUYT, *supra* note 50, at 386 (recounting the state parties’ discussion about the importance of duties); see also NOWAK, *supra* note 6, at 350 (“Freedom of expression, as well as freedom to seek information, is quite capable of violating the rights of others, particularly privacy.”).

<sup>302</sup> As Nowak explains, “as a consequence of the power associated with the influencing of public opinion, the exercise of freedom of expression tends toward concentration and monopolization, which leads to conflicts with the freedom of opinion and expression of others. The power of large media enterprises suppresses the freedom of the press of smaller publishers; the freedom of expression of the owners of media companies competes with that of their editors; and the freedom of expression of the latter conflicts with the great majority of the population, which is unable to procure access to the opinion-shaping media of the modern information society.” NOWAK, *supra* note 6, at 350.

<sup>303</sup> *Id.* at 351.

<sup>304</sup> Oona Hathaway, *Between Power and Principle: An Integrated Theory of International Law*, 72 U. CHI. L. REV. 469, 490 (2005).

*forthcoming 54 Harv. Int'l L.J.* \_\_ (2013)

*Please contact author for an updated version before quoting or citing.*

cannot be understood as “law” without these traditional mechanisms for coercion,<sup>305</sup> scholars have emphasized a variety of ways in which international law nonetheless influences the behavior of states.<sup>306</sup> For Internet intermediaries, as is true for almost all of international law, there is simply no central authority to decide when a particular intermediary’s market presence triggers Article 19 or whether the response of this intermediary is sufficient. In fact, the question of how to enforce the duties that international law imposes directly on non-state actors is even more challenging since this kind of direct duty is so rare in international law. Presumably, as is the case for international law in general, many of these questions will be worked out over time through the norm-generating activities of international institutions and human rights advocates. Enforcement, as well, could occur in the same way that international law influences the behavior of states, through pressure, shame sanctions, socialization, monitoring, and the creation of transnational networks.

The purpose of this section is to suggest that we consider, in addition to these established techniques, a new route for enforcing international law—namely, enforcement through technology itself. As discussed above, code—the architecture of the Internet—can be a highly effective regulatory modality. Like law, markets, and social norms, code affects both what is possible and what is likely online.<sup>307</sup> In making decisions about code, technology companies are routinely making decisions about how to enable and constrain the behavior of states. Indeed, this is nowhere more clear than in the example of China. In applying Lessig’s “code as law” theory to Internet filtering in China, Professors Lee and Liu argue that China’s technological filtering functions as a sort of “law” that regulates behavior.<sup>308</sup> The Great Firewall removes objectionable content originating outside of China automatically and instantaneously, without review or redress.<sup>309</sup> For individuals in China who seek to access blocked information, access is denied even more effectively than if the content were only prohibited by law.<sup>310</sup> These gateway filters make it easier for China to limit expression and information because it makes regulation less costly in terms of time, effort, expertise and expense.<sup>311</sup>

---

<sup>305</sup> JACK L. GOLDSMITH & ERIC A. POSNER, *THE LIMITS OF INTERNATIONAL LAW* 201-02 (2005).

<sup>306</sup> *See, e.g.*, THOMAS M. FRANCK, *FAIRNESS IN INTERNATIONAL LAW AND INSTITUTIONS* (1995); ABRAM CHAYES & ANTONIA HANDLER CHAYES, *THE NEW SOVEREIGNTY: COMPLIANCE WITH INTERNATIONAL REGULATORY AGREEMENTS* (1998); Oona Hathaway & Scott J. Shapiro, *Outcasting: Enforcement in Domestic and International Law*, 121 *YALE L.J.* 252 (2011); Andrew K. Woods, *A Behavioral Approach to Human Rights*, 51 *HARV. INT’L L.J.* 51 (2010); Oona Hathaway, *Between Power and Principle: An Integrated Theory of International Law*, 72 *U. CHI. L. REV.* 469 (2005); Ryan Goodman & Derek Jinks, *How to Influence States: Socialization and International Human Rights Law*, 54 *DUKE L.J.* 621 (2004); Andrew Guzman, *A Compliance-Based Theory of International Law*, 90 *CAL. L. REV.* 1823 (2002); Harold Hongju Koh, *Why Do Nations Obey International Law?*, 106 *YALE L.J.* 2599 (1997).

<sup>307</sup> *See supra* notes 87-101 and accompanying text.

<sup>308</sup> Lee & Liu, *supra* note 99, at 137.

<sup>309</sup> Molly Land, *Google, China, and Search*, 14 *ASIL INSIGHT* 1 (2010), <http://www.asil.org/files/insight100805pdf.pdf>. For content originating within China, the government uses a variety of techniques, including laws that require filtering by ISPs and other Internet service providers, as well as affirmatively spreading disinformation. *Id.*

<sup>310</sup> Of course, China’s filters are not absolute bars. Individuals can obtain otherwise filtered content via circumvention tools and strategies. *See generally* Hal Roberts et al., *2010 Circumvention Tool Usage Report* (October 2010), [http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010\\_Circumvention\\_Tool\\_Usage\\_Report.pdf](http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf). Use of these tools and strategies is costly, however. Even if the costs of routing around filters is not prohibitively expensive, filters that make things even slightly more expensive can disincentivize individuals from pursuing content the government does not want them to see. Further, perfect control is not necessary—the government has only to make expression costly enough that it will deter most of the people most of the time. Derek E. Bambauer, *The Myth of Perfection*, 2 *WAKE FOREST L. REV. ONLINE* 22, 23 (2012) (“leaky Internet censorship works”). This is well illustrated by China. Although the government’s control of the Internet is effective, it is not absolute. Chinese users have access to considerable online content, including some politically sensitive content. Moreover, by allowing some freedom online,

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

Because of the role technology can play in facilitating state compliance with international law, technology companies are not just part of the problem—they are also a critical part of the solution. Technology companies are key allies in the enforcement of Article 19(2) because of their role in the creation and development of code and technical standards.<sup>312</sup> In controlling code, these companies also control a kind of “law.” Moreover, these companies also play a critical role in the development of technical standards. Technical standards can be understood most simply as code that everyone agrees to use. More precisely, they are the “agreed-upon rules structuring information in common formats and establishing communication interfaces that enable interoperability between diverse ICT environments.”<sup>313</sup> One of the most prominent standards organizations is the Internet Engineering Task Force (IETF), a volunteer-based organization aimed at “mak[ing] the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.”<sup>314</sup> Standards are important because they imbue decisions about technology with permanence and create path dependencies, thus making later changes more difficult.<sup>315</sup> Technology companies are often centrally involved in the development of these standards. For example, prominent engineers at leading technology companies have historically played important roles in the decision-making processes of the IETF.<sup>316</sup> Because of the central role they play in creating code and embedding this code in international standards, technology companies are well placed to play a role in enforcing international law through code.

Why should they do so, however? Technology companies do not necessarily have a stellar record when it comes to decisions affecting human rights. Yahoo! was roundly criticized and in fact the subject of a lawsuit for human rights violations as a result of its decision to share user information with the Chinese government that the government used to imprison a dissident.<sup>317</sup> Google’s decision to filter its online search engine in China was viewed as capitulation to a repressive government’s demands. Cisco and other U.S. technology companies have been the subject of heavy criticism in recent years for selling technology and services for monitoring and limiting expression online to countries such as China, Burma, Saudi Arabia, Tunisia, Iran and Yemen, among others.<sup>318</sup> Moreover, it is not clear these companies would be interested in such an

---

China is able to control content that is of most concern while largely avoiding discontent that might become a call for political change. Land, *supra* note 309, at 1.

<sup>311</sup> LESSIG, *supra* note 87, at 56 (“The higher the cost of a regulation, the less likely it will be pursued as a regulation.”).

<sup>312</sup> See Yu, *supra* note 153, at 68 (calling on technology developers to be involved in the process of protecting fair use through code).

<sup>313</sup> DeNardis, *supra* note 89, at 497; see also Brad Biddle et al., *The Expanding Role and Importance of Standards in the Information and Communications Technology Industry*, 52 JURIMETRICS J. 177, 179 (2012) (“ICT products consist of a variety of equipment, devices, and components that work only if they can connect to, and operate with, other equipment, devices, and components often made by other manufacturers.”).

<sup>314</sup> *Mission Statement*, IETF, <http://www.ietf.org/about/mission.html>; see also Ryan, *supra* note 3, at 37.

<sup>315</sup> DENARDIS, *supra* note 90, at 90-91 (“Once adopted, standards permeate technologies made by different manufacturers, and they may endure for long periods of time because of product investments, institutional commitments, and, through network effects, their deep entrenchment in global technology infrastructures.”).

<sup>316</sup> *Id.* at 208 (noting that participants in standards development “usually have the financial backing of salaries from corporate employers supporting their participation” and that at the IETF, individuals “also represent the interests of the institutions funding their involvement”).

<sup>317</sup> See, e.g., Nicholas D. Kristof, Op-Ed, *China’s Cyberdissidents and the Yahoos at Yahoo*, N.Y. TIMES, Feb. 19, 2006, at 13.

<sup>318</sup> See, e.g., HELMI NOMAN & JILLIAN C. YORK, WEST CENSORING EAST: THE USE OF WESTERN TECHNOLOGIES BY MIDDLE EAST CENSORS 2010-2011, [http://opennet.net/sites/opennet.net/files/ONI\\_WestCensoringEast.pdf](http://opennet.net/sites/opennet.net/files/ONI_WestCensoringEast.pdf); BEN WAGNER, EXPORTING CENSORSHIP AND SURVEILLANCE TECHNOLOGY (2012); Richard Winfield & Kristin Mendoza, *Does China Hope to Remap the Internet in Its Own Image?*, 2 J. INT’L MEDIA & ENT. L. 85, 94-97 (2008).



*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

endeavor. Technology companies are, after all, companies that may be more concerned with their bottom line than international human rights values.<sup>319</sup>

There are several reasons why technology companies may be willing partners in supporting freedom of expression and information online. First, despite their varied track record overall, a number of technology companies have in fact been struggling with these issues in a way that reflects a deep commitment to online freedom. For example, although it had initially acceded to Chinese law by censoring its local search engine at *google.cn*, Google decided in early 2010 that it was no longer willing to do this and began redirecting users to its uncensored engine at *google.com.hk*. Clearly, this was motivated at least in part by business interests and security concerns; it noted its decision was a response to a hacking attack originating from China that targeted the Google email accounts of Chinese human rights activists.<sup>320</sup> In part, however, Google's decision also reflected its continued commitment to its informal company motto, "Don't Be Evil." Google has supported and its executives have been active participants in conferences on human rights and freedom of expression online,<sup>321</sup> and it is also one of three technology companies involved in the Global Net Initiative ("GNI"), a multi-stakeholder initiative designed to provide a framework for companies resisting pressure from governments to participate in restrictions on freedom of expression and information as well as mechanisms of accountability, public engagement, and shared learning.<sup>322</sup> Nor is Google alone in its efforts to attend to human rights values. Twitter, for example, rescheduled planned maintenance so as to avoid disrupting the use of the platform in Iran during the election protests.<sup>323</sup>

Second, technology companies may welcome the normative guidance Article 19 offers. Technology companies today are constantly engaged in questions about how to balance their own terms of service, local law, commercial demands, corporate culture, and at times even their own sense of morality. For example, in a dispute several years ago between Google and Turkey after Turkey blocked YouTube because of videos insulting Mustafa Kemal Atturk, Google engaged in a lengthy process of evaluation and negotiation to try to convince Turkey to restore access.<sup>324</sup> As Professor Jeffrey Rosen explains, Google's top management identified and translated potentially offending videos and "set out to determine which ones were, in fact, illegal in Turkey; which violated YouTube's terms of service prohibiting hate speech but allowing political speech; and which constituted expression that Google and YouTube would try to protect."<sup>325</sup> Some within the company took an expansive view of free speech, while others were more conservative. In the end, Google took the position that it would block the videos that violated Turkish law in Turkey but not elsewhere in the world, and it stuck to that position even after the government demanded that the videos be taken down entirely.<sup>326</sup> More recently, Google was embroiled in controversy about the video "Innocence of Muslims," which sparked anti-American protests throughout the Middle East.

---

<sup>319</sup> It is also worth asking why, given this track record, we would want technology companies involved in enforcing international law at all, even if they were willing to do so. I would argue that it is better to have them be part of the process than outside it. Their decisions about technology are going to be informed by values one way or another, and it would seem preferable that these decisions be informed by human rights than simply efficiency or other utility concerns.

<sup>320</sup> Molly Land, *Google, China, and Search*, ASIL INSIGHT, vol. 14, no. 25 (Aug. 5, 2010).

<sup>321</sup> Jim Fruchterman, *Silicon Valley Human Rights Conference*, HUFFINGTON POST BLOG (Oct. 27, 2011, 7:04 PM), [http://www.huffingtonpost.com/jim-fruchterman/silicon-valley-human-rights-conference\\_b\\_1033984.html](http://www.huffingtonpost.com/jim-fruchterman/silicon-valley-human-rights-conference_b_1033984.html).

<sup>322</sup> *About Us*, GLOBAL NETWORK INITIATIVE, <http://www.globalnetworkinitiative.org/about/index.php>.

<sup>323</sup> Maggie Shiels, *Twitter Responds on Iranian Role*, BBC NEWS (June 17, 2009, 8:21 GMT), <http://news.bbc.co.uk/2/hi/technology/8104318.stm>.

<sup>324</sup> See Jeffrey Rosen, *Google's Gatekeepers*, N.Y. TIMES MAGAZINE (Nov. 28, 2008).

<sup>325</sup> *Id.*

<sup>326</sup> *Id.*

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

Google decided to block the video in selected countries, such as Egypt and Libya, but refused to remove it altogether despite pressure from the White House to do so.<sup>327</sup> Article 19 could provide the “deciders” in these companies—those who determine what apps, videos, and posts remain up or are taken down—with useful guidance about how to navigate these complicated questions.

Article 19 could also provide important political “cover” in negotiating the demands of local law and international norms. One of the most difficult challenges technology companies face in a global digital environment is determining when to follow local law and what to do when they know or suspect that the demands of local law are inconsistent with international law. Increasingly, there are calls for companies to resist such demands. Two of the GNI’s Principles on Freedom of Expression, for example, provide as follows:

Participating companies will respect and protect the freedom of expression of their users by seeking to avoid or minimize the impact of government restrictions on freedom of expression, including restrictions on the information available to users and the opportunities for users to create and communicate ideas and information, regardless of frontiers or media of communication.

Participating companies will respect and protect the freedom of expression rights of their users when confronted with government demands, laws and regulations to suppress freedom of expression, remove content or otherwise limit access to information and ideas in a manner inconsistent with internationally recognized laws and standards.<sup>328</sup>

GNI’s Implementation Guidelines provide additional guidance on how to do this, recommending that companies, among other things “encourage governments to be specific, transparent and consistent in the demands, laws and regulations,” and “engage[] proactively with governments to reach a shared understanding of how government restrictions can be applied in a manner consistent with the Principles.”<sup>329</sup> Nonetheless, companies may not feel they have much leverage, rhetorical or otherwise, to resist government demands to comply with local law, even if that law does not comply with international law. Article 19 might provide companies with some authority in this process. Companies might feel they are in a stronger bargaining position if they can argue they are bound by international law themselves to avoid interfering with freedoms of expression and information.

Finally, technology companies may be willing to take an active role in promoting freedom of expression and information as a way of improving their public image. Although companies clearly have significant incentives to comply with demands by governments to enable and facilitate limitations on freedoms of expression and information, there are also incentives that push in the opposite direction for many of these companies. As Professor Tim Wu said in an article about those at Google who decide when to comply with local censorship laws, “One reason there’re good at the moment is they live and die on trust, and as soon as you lose trust in Google, it’s over for them.”<sup>330</sup>

---

<sup>327</sup> Gerry Shih, *White House ‘Innocence of Muslims’ Request Denied: Google Will Not Remove Film from YouTube*, HUFFINGTON POST (Sept. 14, 2012, 6:24 PM), [http://www.huffingtonpost.com/2012/09/14/white-house-innocence-of-\\_n\\_1885684.html](http://www.huffingtonpost.com/2012/09/14/white-house-innocence-of-_n_1885684.html).

<sup>328</sup> *Principles*, GLOBAL NETWORK INITIATIVE, <http://globalnetworkinitiative.org/principles/index.php>.

<sup>329</sup> *Implementation Guidelines*, GLOBAL NETWORK INITIATIVE, <http://globalnetworkinitiative.org/implementationguidelines/index.php>.

<sup>330</sup> Rosen, *supra* note 204.

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

Several technology companies, including Yahoo! and Cisco, have also been the subject of sustained criticism in the press for their sometimes active, sometimes passive complicity in human rights abuses.<sup>331</sup> Google's choice of "Don't Be Evil" as a company motto proved a particularly effective target when the company was criticized for acceding to Chinese censorship demands.<sup>332</sup> Active participation in promoting human rights might be one way for companies to redeem themselves in the eye of the public.

Assuming it is possible to get technology companies on board, what should they do? Technology companies are better positioned than almost anyone else to begin employing the modality of code to enforce international human rights. In other words, because of the central role they play in the creation and dissemination of code and technical standards, these companies are strategically positioned to begin using technology (as opposed to law, markets, or social norms) to promote international human rights. Specifically, companies can do this by making choices that encourage state compliance with human rights law. Although many of the core Internet design principles and protocols such as best efforts routing and end-to-end design already do reflect the values of Article 19, these values are under considerable pressure today, and new questions constantly arise. When faced with choices between standards, those that make it easier and those that makes it harder to violate international human rights law, technology companies should choose a "human right default"—the code or standard that make it more costly for states to violate international human rights law.<sup>333</sup> In other words, the principles articulated in Article 19(2) can be, and should be, embedded directly into code itself.

Article 19 is an appropriate source of guidance for companies that build, program and maintain the technologies of connection for two reasons. First, it is appropriate because it is international law and may bind technology companies in some instances. Second, it is appropriate because in the context of online expression, there are important public interests at stake and third parties might be harmed. In considering how to make choices about software defaults, for example, Professors Jay Kesan and Rajiv Shah argue that defaults in software should be set to maximize efficiency for users, unless one of three circumstances arises: First, defaults might be set to protect individuals if "there is a fundamental societal concern at stake and people are uninformed, misinformed, or not technically sophisticated enough to change the default."<sup>334</sup> Second, defaults might be set to avoid causing "harm to third parties."<sup>335</sup> Third, defaults might ensure compliance

---

<sup>331</sup> *Id.* (noting that "in China in 2004, Yahoo turned over to the Chinese government important account information connected to the e-mail address of Shi Tao, a Chinese dissident who was imprisoned as a result"); see also HELMI NOMAN & JILLIAN C. YORK, WEST CENSORING EAST: THE USE OF WESTERN TECHNOLOGIES BY MIDDLE EAST CENSORS 2010-2011, [http://opennet.net/sites/opennet.net/files/ONI\\_WestCensoringEast.pdf](http://opennet.net/sites/opennet.net/files/ONI_WestCensoringEast.pdf); BEN WAGNER, EXPORTING CENSORSHIP AND SURVEILLANCE TECHNOLOGY (2012).

<sup>332</sup> See, e.g., Hilmar Schmundt & Wieland Wagner, *Great Wall 2.0: How China Leads the World in Web Censorship*, SPIEGEL ONLINE INT'L (May 2, 2008), <http://www.spiegel.de/international/world/great-wall-2-0-how-china-leads-the-world-in-web-censorship-a-551110.html>; Josh McHugh, *Google v. Evil*, WIRED, [http://www.wired.com/wired/archive/11.01/google\\_pr.html](http://www.wired.com/wired/archive/11.01/google_pr.html); Larry Magid, *Google's "Don't Be Evil" Put to the Test*, HUFFINGTON POST (Mar. 24, 2010 3:01 P.M. ET), [http://www.huffingtonpost.com/larry-magid/googles-dont-do-evil-put\\_b\\_511944.html](http://www.huffingtonpost.com/larry-magid/googles-dont-do-evil-put_b_511944.html).

<sup>333</sup> See DENARDIS, *supra* note 92, at 192 ("In cases such as IPv6, designers can engineer, or choose not to engineer, privacy protections into a protocol designed for some other purpose than privacy but that, in its design, raises privacy concerns.").

<sup>334</sup> Jay P. Kesan & Rajiv C. Shah, *Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics*, 82 NOTRE DAME L. REV. 583, 633 (2006).

<sup>335</sup> *Id.*

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

with “existing law and policy.”<sup>336</sup> In addition, both Kesan/Shah and Lessig have emphasized the importance of setting defaults that promote information sharing and transparency.<sup>337</sup>

Although Kesan and Shah were talking about defaults for users,<sup>338</sup> their framework applies equally well when considering defaults for states and the protocols that are agreed upon as international standards. In a general sense, it also makes sense for standards for software code to maximize efficiency—to enable users to find relevant information quickly. This is especially true given the importance of information for the fulfillment of human rights.<sup>339</sup> In situations in which the choice of software defaults might affect freedom of expression and information, however, all of the special circumstances for deviating from this presumption apply. Freedom of expression necessarily implicates important societal interests and affects the interests of third parties, such as others involved in the expression or information exchange. The international community has an interest in ensuring that human rights law is not undermined by technology. In many contexts, users will lack the information needed to be able to change the defaults to protect their own rights or to circumvent the block. Finally, in many contexts, filtering may be invisible—when unable to connect to a particular page, users may not realize this is due to government interference.<sup>340</sup> Given these concerns, when freedom of expression is implicated, the default states and intermediaries chose to embed in software code should favor compliance with human rights law and reflect the principles of Article 19(2).

Full consideration of “human rights defaults”—when and how they might be applied—is beyond the scope of this article and is the subject of another project.<sup>341</sup> Clearly, the idea of human rights defaults necessarily raises a host of questions about whether and if so how code can be used to enforce human rights. In many instances, particularly those that require discretion and balancing, decisions simply cannot be programmed into technology.<sup>342</sup> This does not mean, however, that we cannot build some defaults into the technology of expression that makes it more difficult for states to violate human rights.<sup>343</sup> For example, technology companies might make encrypted communication and “do not track” the defaults in the browsers and email providers they offer. The purpose of this paper, however, is to provide a first step toward this more comprehensive theory by 1) explaining the law and 2) identifying the players. Once we know what international law has to say about new technologies and who needs to be at the table in implementing this law, we can then consider how to put these principles into action.

---

<sup>336</sup> *Id.*

<sup>337</sup> See LESSIG, *supra* note 87, at 181 (in deciding what values we should embrace in code, we should “let that control be obvious to users” because “[o]nly when regulation is transparent is a political response possible); Kesan & Shah, *supra* note 334, at 620-21 (suggesting the use of information forcing penalty defaults where parties are not equally informed as a way of protecting individuals).

<sup>338</sup> For example, Kesan and Shah consider defaults such as values inputted automatically into particular fields or boxes that are or are not checked. Kesan & Shah, *supra* note 334, at 592-93.

<sup>339</sup> See *supra* notes 170-173.

<sup>340</sup> Grimmelman, *supra* note 107, at 1736 (“It may not occur to those regulated by software to think of the man behind the curtain, to conceive of a restrictive design decision as being a decision at all.”).

<sup>341</sup> See Molly Land, *Coding Human Rights* (preliminary draft on file with author).

<sup>342</sup> See Edward W. Felten, A Skeptical View of DRM and Fair Use, Communications of the ACM (Apr. 2003), at 57, 58, <http://delivery.acm.org/10.1145/650000/641232/p56-felten.pdf?key1=641232&key2=0949712501&coll=ACM&dl=ACM&CFID=10297022&CFTOKEN=48631939>.

<sup>343</sup> Yu, *supra* note 153, at 63 (“The fact that the scope and boundaries of these uses, such as the fair use privilege, are uncertain and that software code at the current state of technology may not be able to capture the full range of exceptions and limitations in the copyright system does not mean that we should not build legitimate uses into the DRM systems.”).

*forthcoming 54 Harv. Int'l L.J.* \_\_ (2013)  
*Please contact author for an updated version before quoting or citing.*

## Conclusion

Law always struggles to keep up with technology.<sup>344</sup> Sometimes, existing law is sufficient, and responding to technological developments requires only rereading existing laws; in other instances, new laws are required.<sup>345</sup> International human rights law in the area of freedom of information and expression is more than sufficient to handle the challenges of an information age. In fact, the scope of Article 19(2) is both revolutionary and prescient for a document drafted in the early 1950s. Although no one could have foreseen the Internet in 1950, the state parties who negotiated the ICCPR nonetheless created an instrument that protects it. Moreover, it does so in a technologically neutral way, thus paving the way for the development (and protection) of new and improved means of expressing and communicating information in coming years. Further, Article 19 provides guidance on some of the most pressing issues of Internet governance today—including settlement free peering, quality of service, digital forgetting, informational literacy, the digital divide, and freedom of information. It supports the creation and dissemination of technologies of anonymity and data privacy and casts doubt on gateway filtering, third generation Internet controls and the creation of national cyberzones. As such, Article 19(2) provides the basis for an emerging “international law of the Internet” that can provide normative guidance in debates about the regulation of new technologies.

Applying Article 19(2) to these new challenges also illuminates an important insight about the relationship between international law and technology. Human rights can be affected by the choices we make about software code because code can augment or undermine a government’s ability to regulate. It matters that Article 19(2) protects the means of expression because these means matter, separate and apart from the protection afforded to the content of the communication. Protecting the technologies of connection in this way also fills a critical gap in human rights law. There are many decisions about technological design that affect, but do not themselves violate, international human rights law. Protecting technology allows advocates to intervene in discussions about those decisions. We must attend to these choices because they can have significant consequences for human rights that may not be easily undone after the fact. Recognizing a human right to the medium of expression that explicitly extends to the Internet thus provides an important opportunity to begin considering the role of technology in protecting international human rights.

Finally, this paper is also a call to technology companies to begin taking an active role in the promotion and protection of human rights online. When technology companies occupy such a dominate position in market that their decisions begin to affect freedoms of expression and information, their activities may be directly subject to Article 19—and therefore must be justified according to the principles of Article 19(3). Even aside from this direct effect, however, there are several reasons why technology companies may be particularly effective, and willing, partners in promoting the enforcement of Article 19 principles. Of course, states retain primary responsibility for enforcing Article 19. Technology companies, however, could be important partners, particularly given that states may not be entirely enthusiastic about limiting their own ability to control online

---

<sup>344</sup> Copyright law, in particular, has been forced to adapt in a number of ways. *See generally* Peter S. Menell, *Envisioning Copyright Law’s Digital Future*, 46 N.Y.L. SCH. L. REV. 63 (2002-2003) (discussing the general evolution of copyright law in respond to the challenges of technological developments).

<sup>345</sup> *See* INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS 211 (1995).

*forthcoming 54 Harv. Int'l L.J. \_\_ (2013)*  
*Please contact author for an updated version before quoting or citing.*

expression.<sup>346</sup> Even states committed to greater online freedom are taking steps to ensure their ability to respond to threats to national security and vindicate national interests online.<sup>347</sup> Following the maxim that “code is law,” technology companies could play an important role in enforcing freedom of expression and information online by designing their technology in ways that make it harder for states to violate international human rights.

---

<sup>346</sup> See, e.g., Easton, *supra* note 3 (“Behind the effort [to increase U.N. control of the Internet] are efficient censor machines like China, and autocrats like Russian President Vladimir Putin, who last year declared his desire to establish “international control” of the Internet.”). As Peter Yu has observed, the real question is not how the Internet will affect China, but rather how China will affect the Internet. Yu, *supra* note 208, at 1046.

<sup>347</sup> GOLDSMITH & WU, *supra* note 237, at 150.