

**CONCEPTUALIZING PRIVATE GOVERNANCE IN A NETWORKED
SOCIETY**

Professor Jonathan Peters, University of Kansas*
Professor Brett Johnson, University of Missouri**

Internet law and policy discussions worldwide are converging on the idea that the private sector has a shared responsibility to help safeguard free expression online. This article advances those discussions and makes a significant contribution to the related literature by synthesizing Internet governance concepts with those of content management and with normative theories regarding the social value of freedom of expression—all to the end of better understanding the implications of privately governing speech in a networked society. First, this article examines the emergence of the “networked public sphere” that has distributed the production of expression and renegotiated power relationships among individuals, state actors, and digital intermediaries. Second, to put

* Jonathan Peters is an assistant professor of journalism at the University of Kansas, where he specializes in First Amendment law and media policy. He holds affiliate research positions in the KU Information and Telecommunication Technology Center (exploring Internet governance) and the KU Surveillance Studies Research Center (exploring privacy protections for journalists who use cloud services). Peters is the First Amendment chair of the American Bar Association’s Civil Rights Litigation Committee, and he has written on legal issues for *Esquire*, *The Atlantic*, *Slate*, *Sports Illustrated*, *The Nation*, and *Wired*. Peters has a law degree as well as a Ph.D. in mass communication.

** Brett Johnson is an assistant professor of journalism studies at the University of Missouri, where he teaches mass communication law. He uses traditional legal research methods and both mixed- and multi-method approaches to study the social impacts of the legal and technological regimes governing online communication. Previously, Johnson was an editor of the *Silha Bulletin*, the tri-annual publication of the Silha Center for the Study of Media Ethics and Law at the University of Minnesota, and in 2008 he served as a Rotary Ambassadorial Scholar to Belo Horizonte, Minas Gerais, Brazil, where he studied Brazilian history and blogged about local culture and politics. Johnson has a master’s degree in journalism and a Ph.D. in mass communication.

in concrete terms the idea that intermediaries are regularly conducting “private speech regulation,” this article outlines the chain of digital intermediaries that make up the Internet’s basic infrastructure, shedding new light on the chain by employing a classification system developed originally to discuss different types of intermediaries and how they facilitate speech. This article uses the same classifications to discuss how the intermediaries can constrain speech. It also places these discussions in the context of affirmative First Amendment theory, which says the highest purpose of freedom of expression is to maximize individual participation in the public discourse. Finally, this article concludes by commenting on the history of corporate power over the public discourse and by calling on intermediaries to be transparent regarding their content-governance practices.

I. INTRODUCTION	17
II. CONTENT GOVERNANCE AND THE “NETWORKED PUBLIC SPHERE”	20
<i>A. Agency, Dependence, and Contested Space in Networked Communication.....</i>	<i>24</i>
1. <i>Conceptualizing Content Governance and Individual Agency.....</i>	<i>25</i>
2. <i>Dependence.....</i>	<i>29</i>
<i>B. Interdependence</i>	<i>38</i>
III. THE CHAIN OF DIGITAL INTERMEDIARIES	41
<i>A. Communication Conduits</i>	<i>41</i>
1. <i>Internet Service Providers</i>	<i>42</i>
2. <i>Upstream Providers.....</i>	<i>43</i>
3. <i>Domain Name System</i>	<i>44</i>
<i>B. Content Hosts</i>	<i>47</i>
1. <i>Web-hosting Services.....</i>	<i>48</i>
2. <i>Third-party Platforms.....</i>	<i>49</i>
<i>C. Search and Application Providers</i>	<i>54</i>
1. <i>Search Engines</i>	<i>55</i>
2. <i>Filtering Software.....</i>	<i>57</i>

IV. AGENCY, CONTROL, AND AFFIRMATIVE FIRST AMENDMENT THEORY	58
<i>A. Affirmative Theory</i>	59
<i>B. Synthesis</i>	63
V. CONCLUSION	66

I. INTRODUCTION

In July 2012, a man posted a short film on YouTube dramatizing the life of the Prophet Muhammad filled with “scenes based on slurs . . . repeated by Islamophobes.”¹ The film, titled *Innocence of Muslims*, attracted little attention for months—until an Islamic television station in Egypt aired several scenes.² What happened next remains a matter of national debate. On September 11, 2012, Islamic militants attacked the American diplomatic compound in Benghazi, Libya, injuring ten Americans and killing four others, including the United States ambassador to Libya.³ Many observers, among them the White House press secretary and the United States ambassador to the United Nations, initially said the attack was a demonstration against *Innocence of Muslims*.⁴

It is now believed the attack was part of a larger terrorist plot unrelated to the film,⁵ but protests against the film flared in Egypt,

¹ Robert Mackey & Liam Stack, *Obscure Film Mocking Muslim Prophet Sparks Anti-U.S. Protests in Egypt and Libya*, N.Y. TIMES (Sept. 11, 2012), <http://thelede.blogs.nytimes.com/2012/09/11/obscure-film-mocking-muslim-prophet-sparks-anti-u-s-protests-in-egypt-and-libya/>.

² Michael Joseph Gross, *The Making of Innocence of Muslims: Cast Members Discuss the Film That Set Fire to the Arab World*, VANITY FAIR (Dec. 27, 2012), <http://www.vanityfair.com/culture/2012/12/making-of-innocence-of-muslims>.

³ David D. Kirkpatrick & Steven Lee Myers, *Libya Attack Brings Challenges for U.S.*, N.Y. TIMES (Sept. 12, 2012), <http://www.nytimes.com/2012/09/13/world/middleeast/us-envoy-to-libya-is-reported-killed.html>.

⁴ Gross, *supra* note 2.

⁵ Anne Gearan, *Review of Benghazi attack faults ‘grossly’ inadequate security, leadership failures*, WASH. POST (Dec. 19, 2012), https://www.washingtonpost.com/world/national-security/benghazi-panel-presents-findings-to-lawmakers-makes-recommendations/2012/12/18/9ada6032-495c-11e2-b6f0-e851e741d196_story.html.

Yemen, Iran, and elsewhere.⁶ As the protests continued, Google, the parent company of YouTube, began acting as an arbiter of free speech, restricting access to the video in some places while leaving it unrestricted in others—performing a delicate balancing act normally performed by courts but increasingly familiar to Internet companies.⁷ Notably, Google blocked the availability of *Innocence of Muslims* in Egypt and Libya, citing “the very difficult situation” in both countries.⁸ The company’s general policy is to block content only if it violates local laws or a platform’s terms, or if the company receives a valid court order to block it.⁹ Google conceded that *Innocence of Muslims* did not violate local laws or YouTube’s terms, and neither Egypt nor Libya had ordered that the video be blocked—and yet Google blocked it.¹⁰

In a few parts of the world, Google *did* block *Innocence of Muslims* where it violated local laws. Elsewhere, in the vast majority of sovereigns, Google did not restrict access to the video, even rejecting a request from the White House to reconsider its decision to keep the video online and accessible at all.¹¹ When questioned about its decisions, Google released a statement that read:

⁶ Gross, *supra* note 2.

⁷ Somini Sengupta, *On Web, a Fine Line on Free Speech Across the Globe*, N.Y. TIMES (Sept. 16, 2012), <http://www.nytimes.com/2012/09/17/technology/on-the-web-a-fine-line-on-free-speech-across-globe.html>.

⁸ Claire Cain Miller, *As Violence Spreads in Arab World, Google Blocks Access to Inflammatory Video*, N.Y. TIMES (Sept. 13, 2012), <http://www.nytimes.com/2012/09/14/technology/google-blocks-inflammatory-video-in-egypt-and-libya.html>.

⁹ *Id.*

¹⁰ Susan Benesch & Rebecca MacKinnon, *The Innocence of YouTube*, FOREIGN POL’Y (Oct. 5, 2012), <http://foreignpolicy.com/2012/10/05/the-innocence-of-youtube/>.

¹¹ Declan McCullagh, *White House Pressures Google Over Anti-Islam Video*, CNET (Sept. 14, 2012), http://news.cnet.com/8301-13578_3-57513264-38/white-house-pressures-google-over-anti-islam-video/; Gerry Shih, *Google Rejects White House Request to Pull Mohammad Film Clip*, REUTERS (Sept. 14, 2012), <http://www.reuters.com/article/2012/09/14/us-protests-google-idUSBRE88D1MD20120914>.

We work hard to create a community everyone can enjoy and which also enables people to express different opinions. This can be a challenge because what's OK in one country can be offensive elsewhere. This video—which is widely available on the Web—is clearly within our guidelines and so will stay on YouTube.¹²

To this day, Google has not offered a more detailed explanation of its decisions.¹³

Although the *Innocence of Muslims* controversy might seem exceptional because of the worldwide drama surrounding it, it actually typifies the types of challenges that Internet companies are confronting as they police content on their platforms.¹⁴ Google, Facebook, Twitter, and others, are regularly conducting “private . . . speech regulation”¹⁵ as they “decide what types of content may be posted, whether to remove certain content in response to user requests, whether to remove content that allegedly violates the law, and how to display and prioritize various content types using algorithms.”¹⁶ Such actions—the content decisions that Internet companies make—deserve more scholarly attention. Right now, policy discussions worldwide, from the United States to the European Union, from South America to the United Nations, are converging on the idea that “the private sector has a shared responsibility to help safeguard free expression.”¹⁷

This article advances those discussions and makes a significant contribution to the related literature by synthesizing Internet

¹² *YouTube to be Blocked in Egypt over Anti-Islam Film*, CNET (Feb. 9, 2013), http://news.cnet.com/8301-1023_3-57568533-93/youtube-to-be-blocked-in-egypt-over-anti-islam-film/.

¹³ See, e.g., Jonathan Peters, *Considering and Constraining the Power of Content Hosts*, in *ETHICS FOR A DIGITAL AGE 105* (Bastiaan Vanacker & Don Heider, eds., 2015) (discussing the “Innocence of Muslims” controversy in depth).

¹⁴ *Id.* at 109.

¹⁵ Benesch and MacKinnon, *supra* note 10.

¹⁶ Peters, *supra* note 13, at 105.

¹⁷ Hillary Clinton, *Remarks on Internet Freedom*, The Newseum, Washington, D.C. (Jan. 21, 2010), <http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm>.

governance concepts with those of content management and with normative theories regarding the social value and limits of freedom of expression—all to the end of better understanding the implications of privately governing speech in a networked society. First, this article examines the emergence of the “networked public sphere”¹⁸ that has distributed the production of expression and renegotiated power relationships among individuals, state actors, and digital intermediaries. Second, to put in concrete terms the idea that intermediaries are regularly conducting “private speech regulation,”¹⁹ and to better understand the conceptual discussion of content governance, this article outlines the chain of digital intermediaries that make up the Internet’s basic infrastructure, shedding new light on the chain by employing a classification system developed originally to discuss different types of intermediaries and how they *facilitate* speech.²⁰ This article uses the same classifications to discuss how the intermediaries can *constrain* speech. It also places these discussions in the context of affirmative First Amendment theory, which says the highest purpose of freedom of expression is to maximize individual participation in the public discourse. Finally, this article concludes by commenting on the history of corporate power over the public discourse, and by calling on intermediaries to be transparent regarding their content-governance practices.

II. CONTENT GOVERNANCE AND THE “NETWORKED PUBLIC SPHERE”

The Internet exists on an infrastructure of privately owned websites, servers, and routers, without which the ordinary Internet user would have little or no practical ability to speak or be heard online.²¹ These intermediaries transport, host, and index billions of

¹⁸ YOCHAI BENKLER, *THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM* 212 (Yale University Press 2006), http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf.

¹⁹ Benesch & MacKinnon, *supra* note 10.

²⁰ David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373, 386 (2010).

²¹ *Id.* at 377.

pages of content, enabling them to exercise private power over all manner of speech.²² Correspondingly, that power has made the intermediaries attractive targets for regulators, litigants, and others who want to censor speech that they find disagreeable.²³ This creates a threat to the global system of free expression because intermediaries “are capable of exercising authority over wrongdoers who are otherwise unreachable because [they] are not capable of being identified, are beyond the jurisdiction of the state, or are . . . not amenable to legal pressure.”²⁴ Because intermediaries generally have a fragile commitment to the speech they intermediate, the threat to free speech is very real: “[R]evenue from each marginal customer is small and the cost of a legal defense . . . is high, [so] it is almost always cheaper for the intermediary to remove speech than to expend time or resources contesting even meritless claims.”²⁵

In some respects, of course, this is not a new phenomenon. Private parties have always influenced speech: Neighbors passed information by word of mouth, courier systems distributed news and information written on papyrus, the optical telegraph passed messages across Europe, and newspaper or book editors decided what the public should see and hear.²⁶ All of which means the phenomenon of intermediaries is not new, but the Internet’s extensive reliance on them, and the public’s extensive use of the Internet, has had the effect of significantly amplifying the intermediaries’ power.²⁷ With that in mind, this section examines the emergence of the “networked public sphere”²⁸ that has distributed the production of expression and renegotiated power relationships among individuals, state actors, and digital intermediaries.

²² Benesch & MacKinnon, *supra* note 10.

²³ Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 16 (2006).

²⁴ Ardia, *supra* note 20, at 378–79.

²⁵ Kreimer, *supra* note 23, at 28.

²⁶ Ardia, *supra* note 20, at 382.

²⁷ *Id.* at 378.

²⁸ BENKLER, *supra* note 18, at 212.

This so-called “networked public sphere” has afforded individuals enormous potential simultaneously to create and consume content that is political, cultural, social, and commercial in nature.²⁹ It has “produced a quantitative change in the number of entry points to the sphere of highly distributed expression such that . . . [t]he nation state has lost its complete control as the administrator of the freedom of expression.³⁰ Whereas constitutional and statutory law once dominated the parameters of what citizens could say and the public forums in which they could say it, digital intermediaries have created virtual public forums whose norms are defined by private companies and whose discourse has become difficult for governments to control.

Meanwhile, the power of the intermediaries facilitating the networked communication environment has increased relative to that of individuals, as individuals have grown dependent on the intermediaries to exercise their creative agency.³¹ Thus, although the right of individuals to freedom of expression is still defined vis-à-vis state actors, the functions of freedom of expression—distribution of content and access to information—depend on the digital intermediaries,³² which in turn have enabled more people to enjoy the functions of freedom of expression than at any time in history.³³ As a result, the intermediaries’ capacity to control those

²⁹ Axel Bruns, *BLOGS, WIKIPEDIA, SECOND LIFE, AND BEYOND: FROM PRODUCTION TO PRODUSAGE* 19 (2008).

³⁰ Ejvind Hansen, *Freedom of Expression in Distributed Networks*, 10 *TRIPLEC* 741, 743 (2012), <http://www.triple-c.at/index.php/tripleC/article/view/450>.

³¹ See, e.g., RONALD DEIBERT & RAFAL ROHOZINSKI, *ACCESS CONTROLLED: THE SHAPING OF POWER, RIGHTS, AND RULE IN CYBERSPACE* 7 (Ronald Deibert, John Palfrey, Rafal Rohozinski, & Jonathan Zittrain, eds., 2012); JACK GOLDSMITH & TIM WU, *WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD* 70 (2006); José van Dijck, *Users Like You? Theorizing Agency in User-generated Content*, 31 *MEDIA CULTURE & SOC’Y* 41, 54 (2009).

³² See Laura DeNardis, *Hidden Levels of Internet Control*, 15 *Info., Comm. & Soc’y* 720 (2012); Laura DeNardis, *THE GLOBAL WAR FOR INTERNET GOVERNANCE* 153 (2014).

³³ See generally ELLIOT KING, *FREE FOR ALL: THE INTERNET’S TRANSFORMATION OF JOURNALISM* (2010); BENKLER, *supra* note 18; Bruns, *supra* note 29 (extolling the power that interactive online platforms have given

functions actually threatens the individuals' capacity to realize them.

This article shows that intermediary censorship comes in all shapes and sizes, from state actors blocking user access to search engines, to web-hosting services removing content in response to user complaints. That is notable because the concept of speech constraint, discussed in this section, refers to the constraining effects that entities have on the “relative capacity of individuals to be the authors of their lives,” and “whether the sources of constraint are private actors or public law is irrelevant.”³⁴ Within this framework, individuals have pride of place, and any undue constraint of individual communicative agency is seen as undesirable. Of course, what counts as “undue” is disputed. The networked communication environment has made it possible for individuals to create harmful content (e.g., revenge pornography),³⁵ leading some scholars to call for action by both state actors and digital intermediaries to mitigate the harmful effects.³⁶ The result is that individuals, digital intermediaries, and state actors are in a major struggle to define the norms of freedom of expression in a networked environment³⁷—and the concept of content governance is at the heart of that struggle.

Governing content is about controlling the technologies facilitating individual agency *and* assigning meaning to those technologies,³⁸ which must be analyzed through a “techno-social

individuals not only to access information but also contribute to the creation of cultural products).

³⁴ BENKLER, *supra* note 18, at 141.

³⁵ See Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 346 (2014) (defining revenge porn as “the distribution of sexually graphic images of individuals without their consent.”).

³⁶ See generally AMY GAJDA, *THE FIRST AMENDMENT BUBBLE: HOW PRIVACY AND PAPARAZZI THREATEN A FREE PRESS* (2015); Mary Anne Franks, *Unwilling Avatars: Idealism and Discrimination in Cyberspace*, 20 COLUM. J. GENDER & L. 224 (2011).

³⁷ Manuel Castells, *Communication, Power and Counter-Power in the Network Society*, 1 INT'L J. COMM. 238, 258 (2007).

³⁸ Ganaele Langlois, *Participatory Culture and the New Governance of Communication: The Paradox of Participatory Media*, 14 TELEVISION & NEW MEDIA 91, 100 (2013); LAWRENCE LESSIG, *CODE: VERSION 2.0* 293 (2006).

lens,³⁹ one that recognizes that society and technology are co-determining⁴⁰ and seeks to understand the human values programmed into technology.⁴¹ For those reasons, this section critiques scholarship on individual agency and intermediary control in the context of networked communication, synthesizing those areas to understand how the concepts of control and freedom of expression are being defined. The scope of this analysis is broad and at the institutional level, examining how intermediaries and state actors control content and ultimately shape the norms of freedom of expression. Throughout this analysis, the focus is on user content because it implicates individual agency as well as social and political values, and its potentially harmful nature often triggers removal actions.⁴²

A. Agency, Dependence, and Contested Space in Networked Communication

This section explores scholarship on individual agency and dependence in the context of networked communication. One goal is to capture how and why the increasingly distributed production of expression has renegotiated power relationships among individuals, state actors, and digital intermediaries.⁴³ This renegotiation is recasting the theme of content governance as one of *interdependence* among these three stakeholders, while acknowledging that theoretical power imbalances do exist in certain areas of the networked communication system. The other goal in this section is to highlight that such power imbalances reinforce the argument that the networked communication system is a contested space and that content governance plays a critical role in how state actors, digital intermediaries, and individuals define the norms of networked communication.

³⁹ Hector Postigo, *Cultural Production and the Digital Rights Movement*, 15 INFO. COMM. & SOC'Y 1165, 1171 (2012).

⁴⁰ Leah A. Lievrouw, *New Media, Mediation, and Communication Study*, 12 INFO. COMM. & SOC'Y 303, 310 (2009).

⁴¹ See, e.g., TARLETON GILLESPIE, WIRED SHUT 74 (2007).

⁴² DEIBERT & ROHOZINSKI, *supra* note 31, at 4.

⁴³ van Dijck, *supra* note 31, at 46.

1. *Conceptualizing Content Governance and Individual Agency*

The concept of content governance resides in a web of scholarly literatures.⁴⁴ Therefore, it is useful first to situate the concept within the broader field of private governance of communication. The broader field's literature is far from new. Scholars with roots in the works of philosophers Karl Marx and Michel Foucault, mainly from the critical-cultural vein of the field of mass communication, have theorized that private media companies make up a regime of hegemonic control over individuals' capacity to participate in the public discourse.⁴⁵ In turn, post-positivist scholars have criticized those theories for their lack of empirical proof.⁴⁶ The goal here, then, is to synthesize theories from multiple fields in order to explicate the concept of content governance and to understand its implications.

Content governance is nested in a relatively recent conception of the field of private governance of communication: Internet governance,⁴⁷ a large field that includes data privacy, net neutrality, deep-packet inspection, and the policing of child-abuse images online.⁴⁸ The object of study connecting those dots is "the design and administration of the technologies necessary to keep the Internet operational and the enactment of substantive policy around

⁴⁴ *Id.* at 42.

⁴⁵ See, e.g., DANIEL C. HALLIN, *Hegemony: The American News Media from Vietnam to El Salvador, A Study of Ideological Change and its Limits*, in POLITICAL COMMUNICATION RESEARCH: APPROACHES, STUDIES, ASSESSMENTS 3 (David L. Paletz ed., 1987); ROBERT MCCHESENEY, *DIGITAL DISCONNECT: HOW CAPITALISM IS TURNING THE INTERNET AGAINST DEMOCRACY* (2013).

⁴⁶ See, e.g., Melvin L. DeFleur, *Where Have All the Milestones Gone? The Decline of Significant Research on the Process and Effects of Mass Communication*, 1 MASS COMM. & SOC'Y 85 (1998); Annie Lang, *Discipline in Crisis? The Shifting Paradigm of Mass Communication Research*, 23 COMM. THEORY 10 (2013).

⁴⁷ See, e.g., DENARDIS, *THE GLOBAL WAR FOR INTERNET GOVERNANCE*, *supra* note 32.

⁴⁸ *Id.* at 11; see also Michel van Eeten & Milton Mueller, *Where is the Governance in Internet Governance?*, 15:5 NEW MEDIA & SOC'Y 720 (2012); Malte Ziewitz & Christian Pentzold, *In Search of Internet Governance: Performing Order in Digitally Networked Environments*, 16:2 NEW MEDIA & SOC'Y 306 (2014).

these technologies.”⁴⁹ Generally, the Internet governance field has identified a trend toward the “privatization of authority” in key features of Internet technology,⁵⁰ and a current debate in the field involves the definition of that private authority. Scholarly attention has been dedicated to global institutions governing the Internet, such as the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Governance Forum (IGF), and the World Summit on the Information Society (WSIS).⁵¹ However, scholars have called for the concept of “Internet governance” to apply more broadly to include the “many real-world activities that actually shape and regulate the way the Internet works.”⁵²

That decision is important because if the field were broadened, it would permit scholars to study the role that digital intermediaries play in governing how individuals use networked communication to participate in the global public discourse.⁵³ Intermediaries can be classified into several distinct types, depending on their function in networked communication.⁵⁴ The digital intermediaries discussed in this section are “single-firm industry platforms”⁵⁵ that facilitate networked communication activities.⁵⁶ The platform metaphor is appropriate because the intermediaries support individual users and their agency,⁵⁷ yet the user content published on the platforms is

⁴⁹ DENARDIS, THE GLOBAL WAR FOR INTERNET GOVERNANCE, *supra* note 32, at 6.

⁵⁰ See DEIBERT AND ROHOZINSKI, *supra* note 31, at 12; *see also* REBECCA MACKINNON, CONSENT OF THE NETWORKED: THE WORLDWIDE STRUGGLE FOR INTERNET FREEDOM (2012).

⁵¹ DeNardis, *Hidden Levels of Internet Control*, *supra* note 32; Dawn Nunziato, *Freedom of Expression, Democratic Norms, and Internet Governance*, 52 EMORY L. J. 187 (2003).

⁵² van Eeten & Mueller, *supra* note 48, at 721.

⁵³ See Langlois, *supra* note 38, at 93.

⁵⁴ See *infra* section III.

⁵⁵ KC Claffy & David Clark, *Platform Models for Sustainable Internet Regulation*, 4 J. INFO. POL’Y 463, 466 (2014).

⁵⁶ It is worth mentioning here that within the chain of digital intermediaries discussed in the next section, content hosts—specifically third-party platforms—represent the link in the chain that best connects with this article’s conceptual exploration of content governance and affirmative First Amendment theories. A third-party platform is a type of single-firm industry platform.

⁵⁷ Langlois, *supra* note 38, at 94.

created within frameworks created by the intermediaries.⁵⁸ The companies that own the platforms set the norms of the communicative activities that take place on the platforms. However, the companies do not create such norms in a vacuum. They respond to “pressures from . . . users that they choose to respect”⁵⁹ when creating their terms of use, speech policies, and community standards. Thus, the process of creating speech norms on platforms is dialogical, though the true extent of individuals’ influence over the norms remains an open question.

The concepts of agency and agency facilitation are important to understanding how speech norms are negotiated on platforms. These terms are also central to the meaning of freedom of expression in a networked society, so it is helpful to consider how the network empowers individuals in unique and meaningful ways.⁶⁰ First, the network structure increases agency by increasing the size of the audience that individuals can reach. For example, the structure can turn individual agency into collective action, thereby affording enormous power to social movements.⁶¹ Second, platforms typically offer user-friendly design, ensuring that many individuals with low or moderate levels of technical literacy can contribute to online discourse.⁶² Third, the informal nature of content production and consumption has become normalized.⁶³ As small-scale amateur cultural production is growing more visible

⁵⁸ Joseph B. Walther & Jeong-woo Jang, *Communication Processes in Participatory Websites*, 18 J. OF COMPUTER-MEDIATED COMM. 2, 4 (2012).

⁵⁹ Claffy & Clark, *supra* note 55, at 466.

⁶⁰ DEIBERT & ROHOZINSKI, *supra* note 31, at 3.

⁶¹ Andrew J. Flanagin, Craig Flanagin & Jon Flanagin, *Technical Code and the Social Construction of the Internet*, 12 NEW MEDIA & SOC’Y 179, 182 (2010); Taso Lagos, Ted Coopman & Jonathan Tomhave, ‘Parallel Poles’: *Towards a Theoretical Framework of the Modern Public Sphere, Civic Engagement and the Structural Advantages of the Internet to Foster and Maintain Parallel Socio-Political Institutions*, 16 NEW MEDIA & SOC’Y 398, 409 (2014).

⁶² Ganaele Langlois, *Mapping Commercial Web 2.0 Worlds: Towards a New Critical Ontogenesis*, 14 THE FIBRE CULTURE J. 1, 3 (2009); Flanagin, Flanagin & Flanagin, *supra* note 61, at 184.

⁶³ Ramon Lobato, Julian Thomas & Dan Hunter, *Histories of User-Generated Content: Between Formal and Informal Media Economies*, 5 INT’L J. OF COMM. 899, 909 (2011).

and institutional, individuals are asserting themselves as key players in the network. Fourth, networked communication fully harnesses the “necessarily participatory” nature of the creation of culture.⁶⁴ That is significant because “[h]ow culture is produced is . . . an essential ingredient in structuring how freedom and justice are perceived, conceived, and pursued.”⁶⁵ Thus, freedom of expression, democratic participation, and the creation of culture are all interdependent and active concepts in a system of networked communication.

However, some scholars are skeptical of how much communicative agency individuals really have—and the extent to which such agency makes a difference in public discourse.⁶⁶ These scholars speak of psychological rather than real or empirically observable empowerment among individuals who engage in networked communication.⁶⁷ These scholars argue that individuals have a “sense of agency” or “sense of empowerment,” rather than an actual ability to alter public policy through their participation in the public discourse.⁶⁸

For example, communication scholar Matthew Hindman has lamented the “popular enthusiasm” for the revolutionizing potential of technology, arguing that the enthusiasm “has made a sober appraisal of the Internet’s complicated political effects more difficult.”⁶⁹ Hindman is essentially arguing that it is shortsighted to accept blindly that the Internet is a revolutionary medium that will automatically increase democratic engagement and improve the public discourse simply by increasing access to participate in that discourse. Other factors, such as how that access is controlled and how individuals fluidly define the norms of participating in that

⁶⁴ Postigo, *supra* note 39, at 1166.

⁶⁵ BENKLER, *supra* note 18, at 274.

⁶⁶ See, e.g., MATTHEW HINDMAN, *THE MYTH OF DIGITAL DEMOCRACY* (2009); Ryan J. Thomas, *In Defense of Journalistic Paternalism*, 31 *J. OF MEDIA ETHICS* 86 (2016); Jerome A. Barron, *Access Reconsidered*, 76 *GEO. WASH. L. REV.* 826 (2008).

⁶⁷ Louis Leung, *User-generated Content on the Internet: An Examination of Gratifications, Civic Engagement and Psychological Empowerment*, 11 *NEW MEDIA & SOC’Y* 1327, 1329 (2009).

⁶⁸ Flanagin, Flanagin & Flanagin, *supra* note 61, at 186.

⁶⁹ HINDMAN, *supra* note 66, at 5.

discourse, must be understood before one can assess the true effects of networked communication on the public discourse.

Similarly, in the journalism context, mass communication scholar Brendan Watson has found that Twitter users did not provide alternative perspectives to mainstream news coverage of the 2010 Deep Water Horizon oil spill.⁷⁰ In other words, Twitter may not be so revolutionary a medium in journalism, at least in terms of its ability to further alternative perspectives to major events and thus expand the range of the public discourse. All told, these scholars believe that individual communicative agency should not be thought of in extremes; networked communications are neither revolutionary nor simply normalizing the status quo.⁷¹ Rather, user agency is complex,⁷² and the only way to understand it is through careful, nuanced study.

2. Dependence

The notion of dependence is integral to understanding the concept of content governance. Individuals increasingly depend on the Web as their main source of consuming and sharing information,⁷³ and digital intermediaries increasingly play an indispensable role in facilitating individuals' communicative agency.⁷⁴ In this context, scholars have sought to understand the role that platforms play in "steering" or "channeling" their users' agency.⁷⁵ The process of channeling is at the heart of the meaning of agency and freedom of expression in a networked environment, pitting powerful media against speakers and audiences.⁷⁶ How those concepts are defined affects the very nature of democratic

⁷⁰ Brendan Watson, *Is Twitter an Alternative Medium? Comparing Gulf Coast Twitter and Newspaper Coverage of the 2010 BP Oil Spill*, 43 COMM. RES. 647, 666 (2016).

⁷¹ Scott Wright, *Politics as Usual? Revolution, Normalization and a New Agenda for Online Deliberation*, 14 NEW MEDIA & SOC'Y 244, 257 (2012).

⁷² van Dijck, *supra* note 31, at 42.

⁷³ DAWN C. NUNZIATO, VIRTUAL FREEDOM: NET NEUTRALITY AND FREE SPEECH IN THE INTERNET AGE 2 (2009); DEIBERT & ROHOZINSKI, *supra* note 31, at 7.

⁷⁴ GOLDSMITH & WU, *supra* note 31, at 70.

⁷⁵ van Dijck, *supra* note 31, at 43; Langlois, *supra* note 62, at 102.

⁷⁶ Lievrouw, *supra* note 40, at 307.

discourse online. Indeed, new media scholar Ganaele Langlois believes the agency-dependency balance could “pervert the very democratic ideals of free and unfettered communication on which the Internet is based.”⁷⁷ She is referring to the vision of the Internet captured in 1996 by Internet philosopher John Perry Barlow, who argued in his manifesto “A Declaration of the Independence of Cyberspace” that the Internet should be a realm free from the laws of the world of “flesh and steel.”⁷⁸ As the Internet evolved and became popularized through the invention of the Web, Barlow’s extreme libertarian vision quickly became unrealistic.⁷⁹ Yet the spirit of Barlow lives on among his contemporaries, who readily criticize the instrumental role that private companies play in networked communication. For example, legal scholar Jonathan Zittrain has argued that the private powers that have come to dominate the Internet have both expanded and constrained individuals’ online communicative agency.⁸⁰

Especially germane to this article is the vein of Internet governance research addressing “the evolution of the technical and transactional infrastructures concealed beneath content and how these infrastructures potentially constrain the future of individual civil liberties,” such as freedom of expression.⁸¹ Internet governance scholar Laura DeNardis has written that freedom of expression depends on the Internet’s infrastructure as well as the “policies enacted to preserve both liberty and infrastructure reliability.”⁸² Similarly, legal scholar Jack Balkin has written that the practical ability to speak online depends on an infrastructure of

⁷⁷ Langlois, *supra* note 38, at 95.

⁷⁸ John Perry Barlow, *A Declaration of the Independence of Cyberspace* (1996), <https://projects.eff.org/~barlow/Declaration-Final.html>.

⁷⁹ GOLDSMITH & WU, *supra* note 31; LESSIG, *supra* note 38.

⁸⁰ Jonathan Zittrain, *A History of Online Gatekeeping*, 19 HARV. J. L. & TECH. 253 (2006).

⁸¹ LAURA DENARDIS, *The Social Media Challenge to Internet Governance*, in SOCIETY AND THE INTERNET: HOW NETWORKS OF INFORMATION AND COMMUNICATION CHANGING OUR LIVES, 348 (Mark Graham & William H. Dutton eds., 2014).

⁸² DENARDIS, THE GLOBAL WAR FOR INTERNET GOVERNANCE, *supra* note 32 at 17.

laws, technologies, and corporate practices.⁸³ He says that as our “lives are increasingly dominated by information technology and information flows,” the First Amendment, with its narrow focus on government restrictions of speech, will grow “increasingly irrelevant to the key free speech battles of the future.”⁸⁴

In other words, going forward, democratic values will be as important as ever, but the critical decisions affecting the ability to speak freely online will not involve courts or constitutional law—they will involve technological design, company practices, statutes and regulations, and user activities.⁸⁵ That means digital intermediaries have reached “the front lines of . . . governance issues in cyberspace,”⁸⁶ and studying them is essential to understanding their role in shaping norms of freedom of expression. To that end, this article critiques Professor DeNardis’s three categories of content governance—and it adds a fourth category that reflects the changing networked environment.

i. Discretionary Governance

Commercial intermediaries may voluntarily remove content from their platforms in the absence of a user complaint, a practice called “discretionary” governance.⁸⁷ This form of governance is rare because intermediaries typically remove content in response to complaints or pressure from individuals or governments. Google exercised discretionary governance after *Innocence of Muslims* provoked protests in the Middle East.⁸⁸ Despite its rarity, this governance type illustrates not only an intermediary’s power to

⁸³ Jack M. Balkin, *The Future of Free Expression in a Digital Age*, 36 PEPP. L. REV. 427, 427 (2009).

⁸⁴ *Id.*

⁸⁵ *Id.*

⁸⁶ DENARDIS, THE GLOBAL WAR FOR INTERNET GOVERNANCE, *supra* note 32, at 156.

⁸⁷ *Id.* at 158. DeNardis uses the term “discretionary censorship,” but we replace “censorship” with “governance” for two reasons. The first comes from a desire to highlight the central place of the term “governance” in this analysis and its connection to scholarship on private governance. Second, the term “censorship” is problematic because it typically connotes state control over speech.

⁸⁸ *Id.*

restrict individuals' speech for its own reasons but also the generally limited means for those users to hold an intermediary accountable for abuses of that power. Drawing on legal scholar Yochai Benkler's broad definition of constraint, such unchecked intermediary speech control threatens online public discourse⁸⁹ and therefore needs to be better understood.

Some scholars have adopted the gatekeeping metaphor—once reserved for the editorial processes of journalism⁹⁰—to describe the function of intermediaries as ultimate deciders of what information individuals can access and what user content reaches the public discourse.⁹¹ This metaphor is helpful because gatekeeping exemplifies a “regime of control.”⁹² The challenge for journalists of sifting and curating information and user content supplies an analogy for studying the challenges faced by digital intermediaries. Mass media scholar Jane Singer says that online news sites perform a “secondary gatekeeping” function by judging the value of user content for redistribution.⁹³ The sites' decision-making factors usually include the content's appropriateness as well as redistribution's potential effects on the site's bottom line.

Similarly, mass communication scholars Joshua Braun and Tarleton Gillespie have studied the gatekeeping function of online news sites and their moderation of user comments, which are often “unpolished, wide-ranging, and unpredictable.”⁹⁴ In creating policies for managing “what is sometimes an unruly dialogue,” the sites must ensure that their policies “not only be practical and enforceable, but also balance the economic, professional, and ideological aspirations of the news organization.”⁹⁵ Importantly,

⁸⁹ ETHAN ZUCKERMAN, *Intermediary Censorship*, in ACCESS CONTROLLED: THE SHAPING OF POWER, RIGHTS, AND RULE IN CYBERSPACE 71 (Ronald Deibert et al., eds., 2012).

⁹⁰ See, e.g., PAMELA J. SHOEMAKER & TIMOTHY P. VOS, GATEKEEPING THEORY (2009).

⁹¹ HINDMAN, *supra* note 66, at 12.

⁹² Jane B. Singer, *User-Generated Visibility: Secondary Gatekeeping in a Shared Media Space*, 16 NEW MEDIA & SOC'Y 55, 56 (2014).

⁹³ *Id.*

⁹⁴ Joshua Braun & Tarleton Gillespie, *Hosting the Public Discourse, Hosting the Public*, 5 JOURNALISM PRAC. 383, 383 (2011).

⁹⁵ *Id.* at 384.

“[t]he content policies and their enforcement must toe the line between avoiding legal liability, keeping an eye on the economic bottom line, and some kind of commitment to protecting their users’ freedom of speech and the vibrancy of the public discourse they produce.”⁹⁶ With so many factors to consider, it is challenging for the news sites to distinguish valuable and invaluable speech.⁹⁷

Those realities can be projected onto the broader issue of content governance. Digital intermediaries such as YouTube and Twitter face even more challenging decisions in governing user content compared to those of journalistic institutions, because the boundaries that the digital intermediaries police through content governance are broader and less defined. Digital intermediaries have their own message and image they want to project, but those messages and images compete with the millions of others that individuals publish daily on their platforms. These intermediaries, therefore, must find the proper balance between promoting the speech of their users and protecting their own brands by not allowing speech to become so unruly that it causes an exodus of users.

ii. Delegated Governance

This is the second category of content governance. Public officials who want to suppress speech can pressure intermediaries to do it for them, a practice called “delegated” governance.⁹⁸ The ease and efficiency of using intermediaries to restrict speech offers governments a back door for state-sponsored censorship. Some scholars view this governance type as the most pernicious because of the state actors’ lack of transparency in utilizing it.⁹⁹ In a 2012

⁹⁶ *Id.* at 385.

⁹⁷ *Id.* at 392.

⁹⁸ DENARDIS, *THE GLOBAL WAR FOR INTERNET GOVERNANCE* *supra* note 32, at 213; DeNardis calls this “delegated censorship.” We call it “delegated governance” for the same reasons given in footnote 87.

⁹⁹ Intermediaries, for their part, have been more willing to be transparent about the requests they receive from governments to remove content. *See, e.g., Requests to Remove Content from Governments*, GOOGLE TRANSPARENCY REPORT, <http://www.google.com/transparencyreport/removals/government/?hl=en> (last visited Sept. 7, 2016); *Removal Requests*, TWITTER TRANSPARENCY

collection of essays, digital technology scholars Ronald Deibert and Rafal Rohozinski warned that the biggest threat to free speech today does not come from government efforts to censor or filter content that its citizens or subjects create.¹⁰⁰ Rather, the biggest threat comes from collaborations between governments and commercial platforms to manage user content (e.g., entering into an agreement whereby the platform identifies and removes certain content at the government's behest).¹⁰¹ Deibert and his coauthors argue that hybrid private-public content governance is becoming the new norm for controlling the public discourse.¹⁰² They say that state actors "no longer fear pariah status by openly declaring their intent to regulate and control cyberspace," because they couch their need for control in terms of protecting their citizens from harm.¹⁰³ Meanwhile, intermediaries are likely to heed government pressure to ensure that they can continue to operate in those countries.¹⁰⁴ All of which threatens individuals' chances to engage in democratic discourse via intermediaries.¹⁰⁵

Figure 1 presents a model of delegated content governance in the system of networked communication. Individuals simultaneously publish and consume speech via an intermediary. However, when an individual publishes content a state actor deems objectionable, the actor notifies the intermediary by flagging the content.¹⁰⁶ Intermediary employees or contractors then review the

REPORT, <https://transparency.twitter.com/removal-requests/2014/jan-jun> (last visited Aug. 23, 2016).

¹⁰⁰ See DEIBERT & ROHOZINSKI, *supra* note 31, at 6.

¹⁰¹ An example is the agreement between United Kingdom Prime Minister David Cameron's government and major Internet service providers (ISPs) in the UK to filter by default all content that the government considers "pornographic." See David Cameron, Prime Minister, United Kingdom, Address to Nat'l Soc'y for the Prevention of Cruelty to Child (July 22, 2013), <https://www.gov.uk/government/speeches/the-internet-and-pornography-prime-minister-calls-for-action>).

¹⁰² See DEIBERT & ROHOZINSKI, *supra* note 31, at 11-12.

¹⁰³ *Id.* at 4.

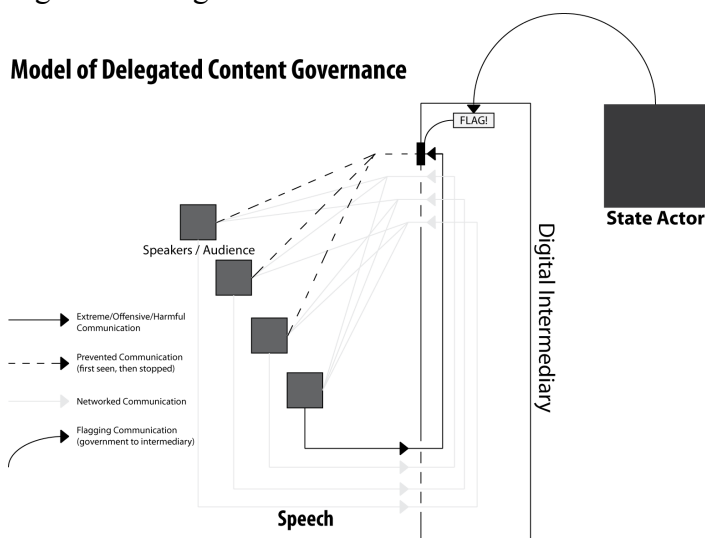
¹⁰⁴ See ZUCKERMAN, *supra* note 89, at 79-80.

¹⁰⁵ MACKINNON, *supra* note 50, at 13-14.

¹⁰⁶ Kate Crawford & Tarleton Gillespie, *What is a Flag for? Social Media Reporting Tools and the Vocabulary of Complaint*, NEW MEDIA & SOC'Y 1, 10 (2014), <http://papers.ssrn.com/sol3/papers.cfm?abstractid=2476464>.

content to determine whether it must be removed because, for example, it violates the law or disrupts the platform's business interests in the state actor's polity. If the intermediary removes the content, that content, represented below by the dashed lines and which was once visible to other individuals, will become invisible via the intermediary.

Figure 1: Delegated Content Governance



iii. Governance Through Legal Compliance

This is the third category of content governance, in which legal violations trigger content governance. For example, in the United States, the Digital Millennium Copyright Act ("DMCA") governs the illegal use of copyrighted material as applied to user content.¹⁰⁷ Under the DMCA's notice-and-takedown regime, rights-holders can give an intermediary notification that their copyrighted works are being published through the intermediary without permission. The intermediary must remove the content within 10 business days to avoid liability for vicarious or contributory infringement.¹⁰⁸

¹⁰⁷ 17 U.S.C. § 512 (2012).

¹⁰⁸ 17 U.S.C. § 512(g)(2)(B) (2012). The intermediary must notify the alleged rights-violators of the takedown (§ 512(g)(2)(C) (2012)), and these authors can file a counter notice with the intermediary claiming that their use of the original work was not infringing (§ 512(g)(3) (2012)).

Outside the United States, governments can notify intermediaries when their hosted content violates local laws and request that the content be removed.¹⁰⁹

This governance type is similar theoretically to delegated governance. However, in practice, this type is distinct because (1) it is generally transparent, and (2) it is usually clear that the content at issue violates statutory law (e.g., a copyright violation through DMCA) or an explicit constitutional test (e.g., the obscenity standard outlined in *Miller v. California*).¹¹⁰

Certainly, governance through legal compliance could be seen as less a matter of private governance than of following the law in the nations where intermediaries operate. However, understanding this type is important because it highlights the intermediaries' legal *and* market incentives to remove or otherwise regulate unlawful content in various countries, including the United States.

iv. Governance by Crowd

This is the fourth category of content governance, and this article adds it to Professor DeNardis's list. A crowd of individuals online can compel digital intermediaries to remove unpopular content, something that legally they could not do in a traditional public forum, such as a public park or town square.¹¹¹ For example, members of a crowd sometimes compel police officers to silence a speaker by threatening violence in response to the person's speech,

¹⁰⁹ An example is the Brazilian judiciary's power to send takedown notices to foreign platforms, such as YouTube, requesting the removal of content that is allegedly defamatory or racist. See Raphael Spuldar, *On the Ground: São Paulo*, INDEX ON CENSORSHIP (Mar. 20, 2013), <http://www.indexoncensorship.org/2013/03/on-the-ground-sao-paulo/>.

¹¹⁰ DENARDIS, *THE GLOBAL WAR FOR INTERNET GOVERNANCE* *supra* note 32, at 213; *see also* *Miller v. California*, 413 U.S. 15, 24 (1973) (holding that content is obscene and lacking First Amendment protection if it appeals to prurient interests, depicts sexual or scatological functions in a patently offensive manner, and lacks serious literary, artistic, political, or scientific value).

¹¹¹ *See, e.g., Cantwell v. Connecticut*, 310 U.S. 296 (1940); *Terminiello v. Chicago*, 337 U.S. 1 (1949); *Gregory v. Chicago*, 394 U.S. 111 (1969); *Cox v. Louisiana*, 379 U.S. 536 (1965); *Edwards v. South Carolina*, 372 U.S. 229 (1963).

an unlawful and unconstitutional practice known as the “heckler’s veto.”¹¹²

This governance type is arguably the most important to understand because mainstream intermediaries, such as Facebook and YouTube, rely on users’ flagging of undesirable content to be made aware of it.¹¹³ Individuals can also pressure intermediaries by publicizing their grievances over undesirable content. Indeed, Facebook removed numerous pages with misogynistic titles (e.g., “Dropkicking sluts in the teeth”) after a group of activists ran a grassroots campaign asking companies to remove their ads from Facebook if the social-networking site refused to remove the misogynistic pages.¹¹⁴

Figure 2 presents a model of governance by crowd. Flagging follows essentially the same process as that for state actors. The main difference is that flagging comes from within the community served by the intermediary instead of from outside the community. Also, rather than deciding whether the flagged content violates the law, intermediaries in Figure 2 must decide whether the flagged content violates their community’s speech standards. That means this governance type involves the pressuring of intermediaries to follow a set of community norms that may amount to a “heckler’s veto” over some speech.¹¹⁵ Reaching a normative conclusion about whether such pressure is desirable requires a greater understanding of the competing values embedded in this governance type: protecting extreme speech and preventing harm.

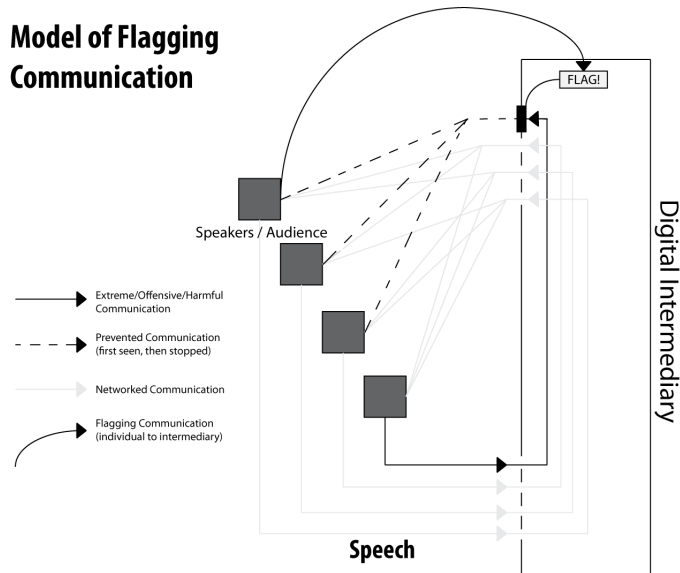
¹¹² *Id.*; see also Brett G. Johnson, *The Heckler’s Veto: Using First Amendment Theory and Jurisprudence to Understand Current Audience Reactions Against Controversial Speech*, 21 COMM. LAW & POL’Y 175, 175–77 (2015).

¹¹³ See Crawford & Gillespie, *supra* note 106.

¹¹⁴ See *Facebook Agreement Statement*, WOMEN, ACTION, & THE MEDIA (May 28, 2013), <http://www.womenactionmedia.org/fbagreement/>.

¹¹⁵ See Johnson, *supra* note 112, at 214; see also ROBERT POST, CONSTITUTIONAL DOMAINS 144 (1995) (contending that the main goal of the First Amendment is to promote “critical interaction” among groups with conflicting opinions and values by preventing the government from invoking community norms to silence extreme speech).

Figure 2: Flagging Communication



B. Interdependence

Understanding the economic pressures that intermediaries face is critical for conceiving a system in which individuals, intermediaries, and state actors are interdependent, rather than one in which individuals are dependent on intermediaries. In the networked-economy context, neither stakeholder can function well without the other.¹¹⁶ Individuals and intermediaries alike demand a participatory culture.¹¹⁷ Motivating production is an important goal for platforms because “giving users more power over content . . . add[s] business value[,]”¹¹⁸ and the creation of user content often generate[s] valuable information as a byproduct.¹¹⁹ That is, intermediaries facilitating user content typically pedal the

¹¹⁶ James Webster, *User Information Regimes: How Social Media Shape Patterns of Consumption*, 104 NW. U. L. REV. 593, 597 (2010).

¹¹⁷ van Dijck, *supra* note 31, at 42.

¹¹⁸ *Id.* at 46; see also Ute Schaedel & Michel Clement, *Managing the Online Crowd: Motivations for Engagement in User-Generated Content*, 7 J. OF MEDIA BUS. STUDIES 17, 19 (2010).

¹¹⁹ Greg Lastowka, *User-Generated Content and Virtual Worlds*, 10 VAND. J. ENT. & TECH. L. 893, 895 (2008).

prospects of fame, entertainment, and play, all in return for commoditizing users' personal data and content.¹²⁰

Scholars have been critical of this “Faustian bargain” that individuals are forced to make.¹²¹ Professor Langlois says it is clear evidence that the power dynamics within commercial participatory media on the Web are “both repressive and productive.”¹²² She laments that “the ease of communication, connection and exploration of one’s interests can only take place through agreeing to terms of service and terms of use that allow for [surveillance of personal data] and the commercialization of user-generated content through advertising.”¹²³ In this system, digital intermediaries that host user content likely have a propensity to view offensive content as risky because of its potential to alienate users and lead to lost subscriptions, while copyright-infringing content creates a risk of legal liability.¹²⁴

Figure 3 presents an interdependence model for a system of networked communication. The arrows represent pressure that each actor puts on the others. Individuals can act as checks on the government through their speech.¹²⁵ However, individuals depend on digital intermediaries to realize that checking function, because the intermediaries, of course, facilitate the speech. At the same time, individuals provide intermediaries a revenue source through commoditization of their content, meaning that intermediaries risk subscription and business losses if their speech restrictions are too great. Governments, meanwhile, can check the individuals' checking power by creating public laws to regulate speech and to influence intermediaries' behavior (e.g., the DMCA).¹²⁶ The United

¹²⁰ Schaedel & Clement, *supra* note 118, at 22–23; van Dijck, *supra* note 31, at 50.

¹²¹ Michael Zimmer, *The Externalities of Search 2.0: The Emerging Privacy Threats when the Drive for the Perfect Search Engine Meets Web 2.0*, 13 FIRST MONDAY 3 (2008).

¹²² Langlois, *supra* note 62, at 11.

¹²³ *Id.* at 2.

¹²⁴ Lobato, Thomas & Hunter, *supra* note 63, at 912.

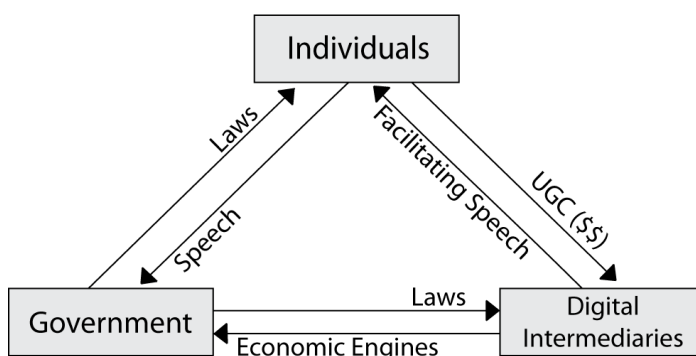
¹²⁵ Vincent Blasi, *The Checking Value in First Amendment Theory*, 2 AM. BAR FOUND. RESEARCH J. 521 (1977).

¹²⁶ For example, in 2008, news organizations filed DMCA takedown requests to have YouTube remove videos that individual users had made, using the news

States Congress also immunized intermediaries from liability for user content through the Communications Decency Act (CDA), a reflection of the intermediaries' power over governments. They are economic engines, according to the CDA's preamble, which states that its intent is "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation."¹²⁷

Figure 3: Interdependence in Networked Communication

Relationships of Interdependence: Powers and Counterpowers



In this interdependent system, the power of speech is only as strong as its counter powers allow it to be, and in the United States, the First Amendment moderates the government's power to constrain speech. So, in a system of networked communication in the United States, digital intermediaries are the entities with the greatest capacity to constrain individuals' speech. But, unlike government power over individuals, intermediary power is not

organizations' footage, to support or criticize candidates in the 2008 elections. Although some of the videos may have constituted fair use of the footage, the DMCA gives intermediaries a strong incentive to remove allegedly infringing content to avoid liability for vicarious infringement. This provision has led some to criticize the DMCA for its potential to unduly punish legitimate speech on matters of public concern. *See, e.g., Campaign Takedown Troubles: How Meritless Copyright Claims Threaten Online Political Speech*, CENTER FOR DEMOCRACY AND TECHNOLOGY (Sept. 2010), https://cdt.org/files/pdfs/copyright_takedowns.pdf.

¹²⁷ 47 U.S.C. § 230 (2012).

necessarily constant. Any number of factors may cause it to wax and wane, such as economic or legal developments, or changing social norms regarding speech.¹²⁸ All of which is to say: just as legal scholars explore how the First Amendment limits the government's power to restrict speech, mass communication scholars must explore how digital intermediaries can act as arbiters of free speech—and how extralegal factors can and do limit their power.

III. THE CHAIN OF DIGITAL INTERMEDIARIES

To put in concrete terms the proposition that intermediaries are regularly conducting “private . . . speech regulation,”¹²⁹ and to better understand the previous section's conceptual discussion of content governance, this section outlines the chain of digital intermediaries that make up the Internet's basic infrastructure. This section sheds new light on the chain by employing a classification system developed by legal scholar David Ardia to discuss different types of intermediaries and how they facilitate speech.¹³⁰ Here, the same classifications are used to discuss how the intermediaries can *constrain* speech. The classifications are: (1) communication conduits, which transport data across the network; (2) content hosts, which “store, cache, or otherwise provide access to third-party content;” and (3) search and application providers, which index and filter content without necessarily hosting it.¹³¹ They are explained and applied in the subparts below.

A. Communication Conduits

These intermediaries facilitate the transport of speech, and typically they have limited control over—and no direct knowledge of—the content of the speech they transport.¹³² In the offline world, examples include telephone companies that intermediate voice traffic and mail carriers that intermediate print materials.¹³³ In the

¹²⁸ See generally LESSIG, *supra* note 38.

¹²⁹ Benesch & MacKinnon, *supra* note 10.

¹³⁰ Ardia, *supra* note 20, at 386.

¹³¹ *Id.* at 386–98.

¹³² *Id.* at 386–87.

¹³³ *Id.*

online world, examples include Internet service providers, upstream providers, and the Domain Name System, all of which intermediate access to content by transporting data across the network.¹³⁴ They have become attractive targets for all kinds of speech constraint.

1. Internet Service Providers

Anyone who uses the Internet must access it through a service provider called an ISP. It is the user's entry point responsible for making web content accessible.¹³⁵ An ISP is supported by backbone providers that simply transmit data and "have no direct relationship with the actors at either endpoint."¹³⁶ Because of the functions it performs, an ISP can operate as a speech constraint in numerous ways. First, even in nations where intermediaries are mostly shielded from liability for user-generated content, some ISPs routinely disconnect users or remove their content rather than expend resources to defend content that has drawn complaints.¹³⁷ Second, governments and rights-holders can pressure ISPs to cut off a user's Internet access after the user has received multiple notifications of copyright infringement.¹³⁸ Third, authoritarian governments have used ISPs to restrict their citizens from accessing the network in their countries, typically to quell dissent.¹³⁹

In 2011, for example, Egyptian president Hosni Mubarak, in response to street protests, ordered the country's six ISPs to go offline, knocking out Internet access for five days.¹⁴⁰ Vodafone,

¹³⁴ *Id.*

¹³⁵ Ardia, *supra* note 20, at 386–87.

¹³⁶ *Id.* at 387.

¹³⁷ *See, e.g.*, Kreimer, *supra* note 23, at 16–27.

¹³⁸ *See, e.g.*, David Kravets, *ISPs Now Monitoring for Copyright Infringement*, WIRED (Feb. 25, 2013), <https://www.wired.com/2013/02/copyright-scofflaws-beware/>.

¹³⁹ Kreimer, *supra* note 23, at 18–21.

¹⁴⁰ Eva Galperin, *Egypt's Internet Blackout Highlights Danger of Weak Links, Usefulness of Quick Links*, ELECTRONIC FRONTIER FOUNDATION (Feb. 8, 2011), <https://www EFF.org/deeplinks/2011/02/egypts-internet-blackout-highlights-danger-weak>.

one of the ISPs, issued a statement saying “Egyptian authorities”¹⁴¹ had demanded that the company “turn down the network totally.”¹⁴² Later, Vodafone issued a statement saying that authorities had used the country’s emergency laws to require the company to send scripted pro-government text messages to its customers.¹⁴³ In other words, the government shut down the Internet, then spread propaganda using a different technology—at once making it difficult for Egyptians to communicate and to verify the claims made in the propaganda.

2. Upstream Providers

A variation on the theme of targeting an ISP is targeting its cousin, an upstream provider. They come in two basic forms: (1) A large ISP that provides Internet access to a local ISP, and (2) a server leased by a third-party platform to host its site.¹⁴⁴ In either form, the provider’s function is to transfer data from the client to the server, creating different chokepoint threats than those created by source and destination ISPs, discussed above.¹⁴⁵ In the chain of intermediaries, the farther from the user a provider is located (upstream providers are at least one layer removed from users), the smaller a provider’s incentive to resist any pressure to censor a user’s speech.¹⁴⁶ The reason is the cost of defending speech tends to be more than upstream providers charge any customer, so they often take the cheaper option of removing content or deactivating users.¹⁴⁷ This can affect not only the targeted user but also any number of collateral users.

¹⁴¹ *Vodafone Forced to Send Pro-Mubarak SMS-es*, NEW DELHI TELEVISION (Feb. 3, 2011), www.ndtv.com/article/world/vodafone-forced-to-send-pro-mubarak-sms-es-83301.

¹⁴² *Egyptian Authorities Asked Vodafone to Cut off Network*, WALL ST. J. (Jan. 28, 2011, 11:11 AM), <http://blogs.wsj.com/davos/2011/01/28/egyptian-authorities-asked-vodafone-to-cut-off-network/>.

¹⁴³ *Id.*

¹⁴⁴ *Free Speech, Upstream Providers* ELECTRONIC FRONTIER FOUNDATION, <https://www.eff.org/free-speech-weak-link#upstream> (last visited Aug. 23, 2016).

¹⁴⁵ *Id.*

¹⁴⁶ *Id.*

¹⁴⁷ Kreimer, *supra* note 23, at 16.

Imagine that a service is hosting a website whose content triggers a takedown request. The service relies on an upstream provider for access to Internet users, and it hosts many sites other than the one whose content triggered the request. In response, the upstream provider could shut down the web-hosting service's entire connection, taking down the site that triggered the takedown *and* innocent bystanders, other sites hosted by the service. That very thing happened in 2009, when the United States Chamber of Commerce attempted to silence a parody site created by "The Yes Men," a group that stages pranks to call attention to corporate misbehavior.¹⁴⁸

Reporters received a press release saying the Chamber would throw "its weight behind strong climate legislation" at a National Press Club event, but the Chamber was not behind the release.¹⁴⁹ It was the work of "The Yes Men," who had also created a parody site to publicize the fake event. The Chamber sent a takedown request to the parody site's upstream provider, claiming the site infringed the Chamber's intellectual property rights by "directly copying the images, logos, design, and layout of the Chamber's . . . official website" ¹⁵⁰ The upstream provider shut down the entire connection to the hosting service, which supported not only "The Yes Men" but also 400 other sites. They were all shut down.

3. Domain Name System

The Domain Name System ("DNS") converts "human-readable host names and domain names, such as Yahoo.com, into the machine-readable, numerical Internet Protocol ["IP"] addresses of a server . . . used to point [a computer] toward the correct [location] on the Internet."¹⁵¹ DNS is the functional equivalent of a

¹⁴⁸ Kate Sheppard, *Chamber Unleashes Lawyers on Yes Men*, MOTHER JONES (Oct. 23, 2009, 12:48 PM), <http://www.motherjones.com/mojo/2009/10/site-sore-eyes-chamber-targets-yes-men-parody-website>.

¹⁴⁹ Kate Sheppard, *The Yes Men Punk the Chamber*, MOTHER JONES (Oct. 19, 2009, 12:31 PM), <http://www.motherjones.com/mojo/2009/10/yes-men-punk-chamber>.

¹⁵⁰ Sheppard, *supra* note 148.

¹⁵¹ *Free Speech Domain Name System (DNS)*, ELECTRONIC FRONTIER FOUNDATION, <https://www EFF.ORG/free-speech-weak-link#dns> (last visited Aug. 23, 2016); *see also* Ardia, *supra* note 20, at 385–86.

directory, making it possible for users to access websites without remembering their IP addresses and server locations.¹⁵² With that in mind, DNS can operate as a speech chokepoint in several ways.

First, ISPs sometimes filter content to restrict access to pornography or websites hosting copyrighted material. ISPs can do so by preventing DNS servers from resolving to the proper IP address a user request for a website. That means the site is still there, but the user cannot access it with the domain name. The problem here is overbreadth: It is often easier for ISPs to block entire domains rather than specific content. In the United Kingdom, for example, the nonprofit Internet Watch Foundation monitors the web for images of child abuse and extreme pornography.¹⁵³ When it finds such images, the organization notifies the relevant ISP or domain-name registrar that a bad actor is using the domain. Then, the ISP or registrar is expected to block or de-register the domain in order to protect users from inadvertent exposure to the offending content. The organization claims it has flagged more than 400,000 web pages in 16 years, resulting in the blocking or de-registering of 100,000 domain names.¹⁵⁴ That approach is blunt and overbroad, as it suppresses a domain's objectionable *and* unobjectionable content.

Second, in authoritarian countries like Iran and China, officials use DNS to suppress speech they find disagreeable; and in progressive countries like Belgium and Norway, officials use DNS to block sites that distribute child pornography.¹⁵⁵ In the United States, too, DNS has disrupted speech. WikiLeaks was inaccessible for a short time in 2010 after the site's DNS provider terminated its agreement with WikiLeaks.¹⁵⁶ The secret-spilling site had been

¹⁵² *Free Speech*, *supra* note 151.

¹⁵³ *About Us*, INTERNET WATCH FOUNDATION, <http://www.iwf.org.uk/about-iwf> (last visited Aug. 23, 2016).

¹⁵⁴ *Child sexual abuse charity CEO: it's time to review, refocus and make a change*, INTERNET WATCH FOUNDATION, <https://www.iwf.org.uk/about-iwf/news/post/364-child-sexual-abuse-charity-ceo-its-time-to-review-refocus-and-make-a-change> (last visited Oct. 1, 2016).

¹⁵⁵ *Free Speech*, *supra* note 151.

¹⁵⁶ Stan Schroeder, *WikiLeaks Downed By Its DNS Service Provider*, MASHABLE (Dec. 2, 2010), <http://mashable.com/2010/12/03/everydns-dns-wikileaks/>.

struggling to fend off a Distributed Denial of Service (“DDoS”) attack after its release of classified United States embassy cables.¹⁵⁷ The DNS provider cited the attack as the reason it terminated its WikiLeaks agreement, saying the attack threatened the services it provided for other users.¹⁵⁸ Without its DNS provider, WikiLeaks existed in the form of partial mirror sites, restricting its ability to operate. Earlier, WikiLeaks had contracted with Amazon Web Services to enhance its “stability and protect itself from DDoS attacks,” but Amazon also dropped WikiLeaks because of pressure from the United States government.¹⁵⁹

Congress later considered DNS blocking to combat intellectual property infringement, through the Stop Online Piracy Act (“SOPA”) introduced in 2011.¹⁶⁰ It would have created a procedure for blacklisting foreign sites that allegedly hosted rights-infringing content. In theory, the SOPA would have protected rights-holders by using DNS to block access to those sites. However, the bill had fatal flaws.¹⁶¹ It empowered the United States attorney general to obtain injunctions against “foreign infringing sites,” defined to include any domain registered outside the U.S. that “facilitates” copyright infringement.¹⁶² The attorney general could obtain the injunction without an adversarial hearing and then order ISPs to block a domain. The attorney general also could sue any party that objected, while non-objecting parties would be immunized.¹⁶³ Thus, the scheme would have created incentives for key elements of the Internet’s infrastructure, including DNS, to act as chokepoints by

¹⁵⁷ *Id.*

¹⁵⁸ *Id.*

¹⁵⁹ Lance Whitney, *Amazon cuts off WikiLeaks*, CNET (Dec. 2, 2010, 8:05 AM PST), http://news.cnet.com/8301-13578_3-20024376-38.html.

¹⁶⁰ Stop Online Piracy Act, H.R. 3261, 112th Cong.. (2011).

¹⁶¹ Jonathan Peters, *Free Expression: Five Questions with Jack Balkin*, HARV. L. & POL’Y REV. (Jan. 10, 2012), <http://web.archive.org/web/20130215152251/http://hlpronline.com/2012/01/free-expression-five-questions-with-jack-balkin/>.

¹⁶² Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011).

¹⁶³ *Id.*

assisting the government in blocking access to certain websites.¹⁶⁴ The SOPA did not pass.¹⁶⁵

B. Content Hosts

These intermediaries play a crucial role in the distribution of speech, and their defining characteristic is that they, unlike conduits, generally have knowledge of and control over the content of the speech they intermediate.¹⁶⁶ In the offline world, examples include bookstores and libraries, which intermediate everything from books to magazines and beyond.¹⁶⁷ In the online world, examples include web-hosting services and third-party platforms, which store, cache, or otherwise provide access to content, operating between primary publishers and their audiences.¹⁶⁸ Most speech that occurs online “is stored on or made available from servers owned by private intermediaries” that decide “when, how, and whether to make that speech available to others.”¹⁶⁹ Web-hosting services allow people to host their own websites, and third-party platforms offer a variety of services, such as social

¹⁶⁴ Peters, *supra* note 161.

¹⁶⁵ *Id.*

¹⁶⁶ Ardia, *supra* note 20, at 398.

¹⁶⁷ *Id.*

¹⁶⁸ Another example worth mentioning here is a payment service provider, which makes it possible for users to send and receive payments online and, in some cases, raise money to support their online speech. Donations through these services can fund everything from political candidates to journalism and poetry. The providers bridge the gaps among senders, financial institutions, and receivers. Thus, the chokepoint threat is that government and private actors can pressure the providers to cut off a speaker’s means of financial support. In 2010, for example, WikiLeaks struggled to cover its operating expenses because PayPal and other payment services bowed to government pressure and stopped processing the organization’s donations. See “Payment Service Providers,” *Free Speech: Only as Strong as the Weakest Link*, ELECTRONIC FRONTIER FOUNDATION, <https://www.eff.org/free-speech-weak-link#payment> (last visited Sept. 9, 2016). We mention this type of provider in a footnote because it is a significant link in the chain of digital intermediaries, but it is beyond this article’s scope to describe *all* of the intermediaries that facilitate communication on the Internet. It is sufficient, we believe, to note the classifications developed by Professor Ardia and provide examples of intermediaries in each one, without purporting to describe every intermediary in the chain.

¹⁶⁹ Ardia, *supra* note 20, at 387–88.

networking, that enable their users to share content. These intermediaries can constrain speech in various ways, and they have become big targets for those who want to suppress speech online.

1. Web-hosting Services

Web-hosting services can be small like Angelfire or large like GoDaddy, and the scope of their services varies significantly, from the hosting of a single webpage with limited file space to the provision of large-scale database support and application-development platforms.¹⁷⁰ Web hosts regularly receive defamation and copyright claims demanding the takedown of hosted material. Some come from companies angry that a host “is providing access to allegedly copyrighted material or to a speaker’s criticism of their corporate practices.”¹⁷¹ Others come from users upset by what they consider defamatory or offensive content. Put differently, some takedown demands are filed in good faith (e.g., a photographer demanding that a site remove a copyrighted image used without authorization and not constituting fair use), while others wear the scarlet letter of censorship (e.g., a company demanding that a site remove content with the intent of chilling speech). The line between the two can be thin.

In 2006, for example, an anonymous blogger called Spocko published audio clips from a talk-radio program on KSFO-AM in order to criticize what the blogger characterized as the hosts’ “racially insensitive and religiously intolerant rhetoric.”¹⁷² In response, ABC Inc., which owns the radio station and the copyrights to its content, sent a letter to Spocko’s web host claiming that the clips violated the company’s copyrights and demanding that the host direct Spocko to take down the clips.¹⁷³ The web host shut down Spocko’s blog, prompting Spocko to find a different host. Then, the Electronic Frontier Foundation, a

¹⁷⁰ “Webhosting Services,” *Free Speech: Only as Strong as the Weakest Link*, ELECTRONIC FRONTIER FOUNDATION, <https://www.eff.org/free-speech-weak-link#webhost> (last visited Aug. 23, 2016).

¹⁷¹ *Id.*

¹⁷² “ABC v. Spocko,” DIGITAL MEDIA LAW PROJECT, (Feb. 22, 2008), http://www.dmlp.org/threats/abc-v-spocko#node_legal_threat_full_group_description.

¹⁷³ *Id.*

nonprofit digital-rights organization, sent a letter to ABC stating that Spocko's use of the clips—for the purpose of criticizing the radio program—constituted fair use.¹⁷⁴ The letter also stated that “ABC/KSFO's complaints amount to nothing more than an attempt to silence an effective critic,” warning ABC that it could be liable under the Digital Millennium Copyright Act for misrepresenting a copyright claim.¹⁷⁵ In the end, neither side filed a lawsuit, ABC never responded to the EFF's letter, and Spocko moved his blog to a new host that promised not to restrict his expressive activities.¹⁷⁶

2. Third-party Platforms

Google, Facebook, YouTube, and Twitter are examples of third-party platforms that offer a variety of services that enable their users to share content.¹⁷⁷ When a blogger covering government corruption speaks to the world, he might do so via a blog-hosting service like Tumblr.¹⁷⁸ When an activist organizes a protest, she might do so via a social-networking site like Facebook.¹⁷⁹ When a citizen journalist shares photos and videos of a major press conference, he might do so through hosting sites like Flickr or YouTube.¹⁸⁰ Indeed, for most people, third-party platforms are their principal means of online and public communication.¹⁸¹ The chokepoint here stems from the reality that the employees who develop and enforce the platforms' content rules have greater “power over who gets heard around the globe

¹⁷⁴ *Id.*

¹⁷⁵ *EFF Tells Radio Station To Back Off Blogger*, ELECTRONIC FRONTIER FOUNDATION (SEPT. 28, 2016), <https://www.eff.org/es/press/mentions/2007/07/18-24>.

¹⁷⁶ “Spocko and ABC/KSFO,” ELECTRONIC FRONTIER FOUNDATION, <https://www.eff.org/cases/spocko-and-abc-ksfo> (last visited Aug. 23, 2016); DIGITAL MEDIA LAW PROJECT, *supra* note 172.

¹⁷⁷ Ardia, *supra* note 20, at 388.

¹⁷⁸ *Id.*

¹⁷⁹ *Id.*

¹⁸⁰ *Id.*

¹⁸¹ See generally E. Newland, et. al., *Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users*, CENTER FOR DEMOCRACY AND TECHNOLOGY and the BERKMAN CENTER FOR INTERNET AND SOCIETY (Sept. 20, 2011), http://cyber.law.harvard.edu/publications/2011/account_deactivation.

than any politician or bureaucrat.”¹⁸² The rules they develop, along with how they enforce those rules, provide as much a study of arbitrary reasoning as a study of principled reasoning. A full exploration of the practices of third-party platforms is beyond the scope of this article, but consider those of Facebook—the largest third-party platform in the world, in terms of monthly active users.¹⁸³

Many hundreds of content moderators work around the clock for Facebook to review user complaints about posts that contain nudity, hate speech, pornography, threats, violence, and other supposed evils—working from offices in the United States, Ireland, and India, among others.¹⁸⁴ The complaints are voluminous. Each week, Facebook receives more than two million requests to remove content.¹⁸⁵ How the company responds to those requests has changed over time, and Dave Willner’s career at Facebook provides a case study in how and why the changes took place. After a few years working in the help center and on content policy, Willner, then twenty-eight years old, became head of Facebook’s content policy team—just six employees at the Menlo Park headquarters.¹⁸⁶ Facebook had no content rules when Willner joined that team, so he attempted to write the rules himself.

He began by using university codes as models, and then, frustrated by their vagueness, he sought inspiration from John Stuart Mill’s writings and the First Amendment.¹⁸⁷ Willner learned that the latter required a presumption against prior restraints of speech and speech should only be “banned only when it is intended—and likely—to incite imminent violence or lawless

¹⁸² Jeffrey Rosen, *The Delete Squad: Google, Twitter, Facebook and the New Global Battle over the Future of Free Speech*, THE NEW REPUBLIC (Apr. 29, 2013), <http://www.newrepublic.com/article/113045/free-speech-internet-silicon-valley-making-rules>.

¹⁸³ *Facebook Remains the Largest Social Network in Most Major Markets*, EMARKETER (Apr. 8, 2016), <http://www.emarketer.com/Article/Facebook-Remains-Largest-Social-Network-Most-Major-Markets/1013798>.

¹⁸⁴ Rosen, *supra* note 182.

¹⁸⁵ *Id.*

¹⁸⁶ *Id.*

¹⁸⁷ *Id.*

action.”¹⁸⁸ However, he also learned that European free-speech values were more limited, forbidding, for example, speech that “offends the dignity of members of a protected class and lowers their standing in society.”¹⁸⁹ Ultimately, Willner decided that both regimes were too subjective—in large part because his content moderators, in offices around the world, brought to their roles different cultural norms and experiences. They needed rules that focused on “concrete, easily categorized actions.”¹⁹⁰

To that end, Facebook hired a consulting firm to produce what became the “Operations Manual for Live Content Moderators,” intended to help the diverse street-level moderators respond to removal requests.¹⁹¹ The seventeen-page manual was leaked in 2012 to Gawker, and it drew wide criticism for its specificity and dubious distinctions.¹⁹² Divided into categories like “Sex and Nudity,” “Hate Content,” and “Graphic Content,” it required content moderators to delete, among other things: “Sex toys or other objects, but only in the context of sexual activity,” “Images of drunk and unconscious people, or sleeping people with things drawn on their face,” and “Photoshopped images of people, whether negative, positive or neutral.”¹⁹³ The manual also required moderators to escalate some requests to Willner’s team at headquarters: credible threats against people, suicidal content, incitements to imminent lawless action, and material related to “international compliance,” such as holocaust denial, which is unlawful in some countries.¹⁹⁴ Willner and his team operated as a court of last resort.

Applying those rules proved difficult, and the company’s “zealousness in scrubbing users’ content” produced a number of

¹⁸⁸ *Id.*; see generally *Near v. Minnesota*, 283 U.S. 697 (1931).

¹⁸⁹ Rosen, *supra* note 182.

¹⁹⁰ *Id.*

¹⁹¹ *Id.*

¹⁹² Adrian Chen, *Inside Facebook’s Outsourced Anti-Porn and Gore Brigade, Where ‘Camel Toes’ are More Offensive Than ‘Crushed Heads,’* GAWKER (Feb. 16, 2012), <http://gawker.com/5885714/inside-facebooks-outsourced-anti-porn-and-gore-brigade-where-camel-toes-are-more-offensive-than-crushed-heads>.

¹⁹³ *Id.*

¹⁹⁴ *Id.*

controversies.¹⁹⁵ First, in February 2011, Facebook removed a drawing posted by the New York Academy of Art that depicted a topless woman.¹⁹⁶ Outraged, the school issued a statement: “[We] find it difficult to allow Facebook to be the final arbiter—and online curator—of the artwork we share with the world.”¹⁹⁷ Facebook said the removal was a mistake and apologized. Second, in April 2011, Facebook removed a photo of two gay men kissing, and the company was accused of homophobia.¹⁹⁸ Officials said the removal was a mistake and apologized.¹⁹⁹ Third, in February 2012, a group of women gathered at Facebook’s headquarters to protest the regular removal of breastfeeding photos.²⁰⁰ Facebook said the removals were a mistake and apologized, revising the company’s content rules to clarify that users, generally, were permitted to post breastfeeding photos.²⁰¹

Amid these and other controversies, Facebook ended its relationship with the consulting firm and abandoned the manual, and Willner “redoubled his efforts to minimize the opportunities for subjective verdicts by his first responders.”²⁰² Eventually, those efforts led to the adoption of new “Community Standards” governing “what type of expression is acceptable, and what type of content may be reported to us and removed.”²⁰³ Those standards were tested acutely in September 2012, when Facebook refused to block the sharing of *Innocence of Muslims*. Willner concluded that the video complied with Facebook’s standards because it contained

¹⁹⁵ *Id.*

¹⁹⁶ Adrian Chen, *How to Get Boobs on Facebook*, GAWKER (Feb. 19, 2011), <http://gawker.com/5765057/how-to-get-a-boob-on-facebook>.

¹⁹⁷ *Id.*

¹⁹⁸ Adrian Chen, *Facebook Apologizes for Censoring Gay Kiss*, GAWKER (Apr. 19, 2011), <http://gawker.com/5793536/facebook-apologizes-for-censoring-gay-kiss-picture>.

¹⁹⁹ *Id.*

²⁰⁰ Ryan Tate, *Why Moms Are Breastfeeding In Facebook’s Face*, GAWKER (Feb. 7, 2012), <http://gawker.com/5883135/why-moms-are-breastfeeding-in-facebooks-face>.

²⁰¹ *Id.*

²⁰² Rosen, *supra* note 182.

²⁰³ “Facebook Community Standards,” FACEBOOK, <https://www.facebook.com/communitystandards> (last visited Aug. 23, 2016).

attacks on an institution, Islam, rather than a group, Muslims.²⁰⁴ That distinction was critical under the new standards, which stated: “[p]eople can use Facebook to challenge ideas, institutions, events, and practices,” but Facebook will remove speech “which includes content that directly attacks people based on their . . . religion.”²⁰⁵

Today, Facebook is evolving yet again as a potential chokepoint.²⁰⁶ It is partnering with news organizations to enable them to post stories directly to Facebook—instead of providing access to the content through a link.²⁰⁷ The partnerships may generate good money for cash-strapped news sites, but they give Facebook the power to play kingmaker, to decide “which news organizations [will] thrive and which will die.”²⁰⁸ Moreover, the partnerships give the social-networking site greater control, at least technologically, over some news content. As one commentator put it, “In the future, it may not be the *New York Times* that the White House pressures to stop publication of a . . . story. [Officials] may . . . head straight for who . . . controls whether millions will actually see the next explosive national security investigation: Facebook.”²⁰⁹ That control stems from the company’s content moderation and its algorithms that determine what users see in their feeds. The resulting chokepoint risks are considerable, as the same commentator explains:

²⁰⁴ Rosen, *supra* note 182.

²⁰⁵ FACEBOOK, *supra* note 203.

²⁰⁶ One issue Facebook is confronting as of the writing of this article is how to manage users’ livestreaming video, through the platform’s new Facebook Live feature. It has been used to stream the sniper ambush of police officers in Dallas and the police killing of Philando Castile in Minnesota, among other events. As the *New York Times* recently reported, “Now Facebook must navigate when, if at all, to draw the line if a live video is too graphic, and weigh whether pulling such content is in the company’s best interests if the video is newsworthy.” See Mike Isaac and Sydney Ember, *Live Footage of Shootings Forces Facebook to Confront New Role*, N.Y. TIMES (Jul. 8, 2016), <http://www.nytimes.com/2016/07/09/technology/facebook-dallas-live-video-breaking-news.html>.

²⁰⁷ Trevor Timm, *The Most Concerning Element of Facebook’s Potential New Power*, COLUM. JOURNALISM REV. (Apr. 13, 2015), http://www.cjr.org/criticism/facebook_news_censorship.php.

²⁰⁸ *Id.*

²⁰⁹ *Id.*

News organizations have always been at risk of bending to the will of their advertisers—and history is replete of examples of them doing just that. But the changing dynamics around Facebook are of a different order. Standard Oil or Pfizer or General Motors never had the power to ensure millions of *New York Times* subscribers would not get their paper the next day. Yet with one click, Facebook could pull off the modern-day equivalent.²¹⁰

Of course, Facebook is not the only third-party platform conducting speech regulation. Google, Twitter, and Instagram, among others, are doing so, too, as they develop and enforce their own content rules.²¹¹ Facebook is highlighted here as an exemplar, to demonstrate how the “sovereigns of cyberspace”²¹² are writing a major chapter in the story of free speech—how they are capable of operating, for any number of reasons, as chokepoints separating a speaker from its audience.²¹³

C. Search and Application Providers

These intermediaries, by indexing or filtering content, allow people to locate and sort through the digital world’s voluminous information and to direct their attention to that which interests them.²¹⁴ In the online world, examples include search engines and filtering software.²¹⁵ In the offline world, close analogs are not apparent, but the closest would be telephone directories, stock prices, and bond ratings.²¹⁶ In any case, search engines can be major chokepoints because of their importance to Internet users, who generally must employ one to get around the Web. Filtering

²¹⁰ *Id.*

²¹¹ See, e.g., “The Twitter Rules,” TWITTER, <https://support.twitter.com/articles/18311> (last visited Aug. 23, 2016); “Community Guidelines,” INSTAGRAM, <https://help.instagram.com/477434105621119/> (last visited Aug. 23, 2016).

²¹² MacKinnon, *supra* note 50.

²¹³ Sengupta, *supra* note 7.

²¹⁴ Ardia, *supra* note 20, at 389.

²¹⁵ *Id.*

²¹⁶ *Id.*

software, by contrast, is a chokepoint by design. The exact nature and extent of their capacities to suppress speech vary. Like content hosts, and unlike communication conduits, these providers have limited knowledge of—and limited control over—the content of the speech they intermediate, insofar as search engines and filtering software select search results based on computer algorithms *and* thematic preferences representing the engineers' judgments about which information to present and how to do so.²¹⁷

1. Search Engines

Efforts to manipulate search results can threaten the principle of search neutrality: the idea that users should get the results they want rather than the results an interested party wants them to see.²¹⁸ Those efforts are fueled by governmental and non-governmental actors. First, some authoritarian governments block entire search engines or force them to blacklist certain queries—all to limit access to content that does not support the government's official version of reality. Until 2010, for example, Google agreed to censor its results in Mainland China.²¹⁹ When the company ended that agreement, Google began routing its Chinese traffic through Hong Kong servers, beyond the reach of Beijing's censorial laws.²²⁰ Mainland users could still use Google, but the connection broke if they searched for certain terms.²²¹ It was no longer Google doing the censoring, though; it was the Chinese government and the so-called Great Firewall of China.²²² Notably, in 2012, Google added a feature to its Chinese homepage that warned users when

²¹⁷ Eugene Volokh, *First Amendment Protection for Search Engine Search Results*, VOLOKH CONSPIRACY (May 9, 2012, 2:37 PM), <http://www.volokh.com/2012/05/09/first-amendment-protection-for-search-engine-search-results/>.

²¹⁸ *Id.*

²¹⁹ Ryan Singel, *Google, China and Censorship: A Wired.com FAQ*, WIRED (Apr. 2, 2010, 9:47 AM), <http://www.wired.com/2010/04/google-china-and-censorship-a-wiredcom-faq>.

²²⁰ Bianca Bosker, *Google Shuts Down China Search, Redirects Users To Hong Kong*, HUFFINGTON POST (May 23, 2010, 9:11 AM), http://www.huffingtonpost.com/2010/03/22/google-leaves-china-googl_n_508639.html.

²²¹ *Id.*

²²² *Id.*

they entered sensitive terms that their connection might break.²²³ The feature, which Google removed one year later without comment, also suggested alternative terms for users to try that would not break the connection.²²⁴

Second, industry groups and individuals have realized the potential for search engines to choke off speech. Groups that lobby for copyright enforcement, such as the Motion Picture Association of America, have taken on torrent search indices that are used to distribute files over the Internet at fast speeds, and individuals have claimed that search results that are defamatory or otherwise illegal must be removed.²²⁵ For individuals, especially, the chief concern is the Internet's long memory and the "world of Big Data and ever more powerful search engines, in which it seems almost everything is permanently recorded and accessible to almost anyone."²²⁶ These are the concerns breathing life into the "Right to be Forgotten," recognized in Argentina and the European Union.²²⁷ More generally, such concerns are challenging news outlets in unique ways, even in countries where no "Right to be Forgotten" is recognized.

In the United States, for example, news organizations frequently receive requests to remove archived stories from people who wish to escape the pall cast over them by negative coverage.²²⁸ News organizations have little interest in rewriting history, but some, to moderate the Internet's long memory, have agreed in limited circumstances to insert a line of code into online stories to prevent them from being found by search engines. In other words, the stories "can still be found in the paper's digital archive, just as

²²³ Joe McDonald, *Google Helps Chinese Avoid Censorship*, USA TODAY (Jun. 1, 2012, 8:59 AM), <http://usatoday30.usatoday.com/tech/news/story/2012-06-01/google-china-censorship/55326416/1>.

²²⁴ *Id.*

²²⁵ "Search Engines," *Free Speech: Only as Strong as the Weakest Link*, ELECTRONIC FRONTIER FOUNDATION, <https://www.eff.org/free-speech-weak-link#search> (last visited Aug. 23, 2016).

²²⁶ Bill Keller, *Erasing History*, N.Y. TIMES (Apr. 28, 2013), <http://www.nytimes.com/2013/04/29/opinion/keller-erasing-history.html>.

²²⁷ See generally Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88 (2012).

²²⁸ Keller, *supra* note 226.

they can be found in bound volumes at the local library, but they do not show up on Google.”²²⁹ The implications are significant: without an easy way to find digital information, it might as well not exist.

2. Filtering Software

In its most basic form, filtering software protects users from web-borne malware or spam, and screens out unwanted content.²³⁰ Public schools and libraries use filters to comply with laws requiring them to deny access to adult-oriented or sexually explicit material. Filters, then, are designed to be chokepoints—but their effects can go beyond their design. Indeed, they are susceptible to the problems of overblocking and underblocking.²³¹ An overblocking filter screens out wanted content, and an underblocking filter fails to screen out unwanted content.²³²

Consider, as an example, a 2012 incident at a Missouri public high school. While conducting research at school, students discovered they could access websites for anti-gay organizations but not websites for pro-gay organizations.²³³ They also discovered they could access the *Bowers v. Hardwick* opinion, in which the Supreme Court upheld a statute criminalizing sodomy, but they could not access the *Lawrence v. Texas* opinion, in which the Supreme Court invalidated state laws criminalizing sodomy.²³⁴ The culprit: the school’s filtering software, which placed pro-gay organizations in its “sexuality” category, designed to screen out pornography.²³⁵ Meanwhile, the software placed anti-gay organizations in the “religion” category, subject to no

²²⁹ *Id.*

²³⁰ See generally Phillip B. Stark, *The Effectiveness of Internet Content Filters*, 4 J. L. & POL’Y FOR THE INFO. SOC’Y 411 (2008).

²³¹ *Id.* at 415.

²³² *Id.*

²³³ Michael Winerip, *School District Told to Replace Web Filter Blocking Pro-Gay Sites*, N.Y. TIMES (Mar. 26, 2012), <http://www.nytimes.com/2012/03/26/education/missouri-school-district-questioned-over-anti-gay-web-filter.html>.

²³⁴ *Id.*

²³⁵ *Id.*

restrictions.²³⁶ As an American Library Association official told the *New York Times*, “[F]ilters are a new version of . . . pulling books off the shelf. The difference is, this is much more subtle and harder to identify.”²³⁷

IV. AGENCY, CONTROL, AND AFFIRMATIVE FIRST AMENDMENT THEORY

The previous two sections discussed content governance conceptually and in concrete terms through an evaluation of the chain of digital intermediaries and of the proposition that they are regularly conducting “private . . . speech regulation.”²³⁸ This section places those discussions in the context of affirmative First Amendment theories, which generally contend that freedom of expression’s highest purpose is to maximize individual participation in the public discourse. Content governance, as a subfield of Internet governance, deserves the sustained attention of the even wider field of mass communication law, consistent with comments from legal scholar Enrique Armijo that networked-communication issues “now establish the frame within which all of our public policy and academic debates concerning communications law and policy take place.”²³⁹ Connecting content governance and mass communication law is difficult, though, and several guidelines must be established to synthesize those fields. Although the traditional practice of mass communication law research has been to draw normative conclusions about freedom-of-expression issues based on a single theoretical framework,²⁴⁰ it is unwise to draw such conclusions about content governance until the concept can be evaluated from the perspective of multiple theories of freedom of expression. In other words, scholars must be cautious to avoid the pitfalls of advancing normative conclusions unmoored from diverse First Amendment jurisprudence.

²³⁶ *Id.*

²³⁷ *Id.*

²³⁸ Benesch & MacKinnon, *supra* note 10.

²³⁹ Enrique Armijo, *Communication Law, Technological Change, and the New Normal*, 19 COMM. L. & POL’Y 401, 402 (2014).

²⁴⁰ Matthew Bunker and David Perry, *Standing at the Crossroads: Social Science, Human Agency and Free Speech Law*, 9 COMM. L. & POL’Y 1 (2004).

To that end, the starting point is to recognize, again, that digital intermediaries are powerful institutions that can restrict the speech that individuals publish on their platforms. That recognition permits content governance to be assessed using affirmative theories of freedom of expression, such as legal scholar Alexander Meiklejohn's self-governance theory,²⁴¹ the "new realist" theories of the 1990s,²⁴² and emerging theories stressing the maximization of individual participation in a networked communication environment.²⁴³ The common thread running through these theories is that they all acknowledge the control that powerful non-governmental institutions (e.g., media corporations) can exercise over individuals' participation in the public discourse. Notably, the theories all acknowledge the potential of state actors to increase the individuals' power in relation to that of the institutions. The affirmative theories propose various policies that state actors can adopt to advance the maximization of individual participation in the public discourse. Proponents of negative theories of freedom of expression,²⁴⁴ which emphasize freedom from government interference rather than freedom to achieve specific substantive outcomes, have criticized those policies. But it is possible, nonetheless, to accept the premise that media institutions have a great deal of power to control the public discourse. This premise is the foundation for understanding the interdependent nature of content governance from the perspective of legal theory.

A. Affirmative Theory

Affirmative theories of freedom of expression find their roots in Professor Meiklejohn's self-governance theory.²⁴⁵ Meiklejohn

²⁴¹ ALEXANDER MEIKLEJOHN, *FREE SPEECH AND ITS RELATION TO SELF-GOVERNMENT* (1948).

²⁴² See, e.g., CASS SUNSTEIN, *DEMOCRACY AND THE PROBLEM OF FREE SPEECH* (1993); Owen Fiss, *Why the State?*, 100 HARV. L. REV. 781 (1987).

²⁴³ See e.g., Marvin Ammori, *First Amendment Architecture*, 2012 WIS. L. REV. 1 (2012); Jack Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. REV. 1 (2004); Nunziato, *supra* note 51.

²⁴⁴ Ronald Cass, *The Perils of Positive Thinking: Constitutional Interpretation and Negative First Amendment Theory*, 34 UCLA L. REV. 1405 (1987).

²⁴⁵ Meiklejohn, *supra* note 241.

argued that the First Amendment's central purpose was not found in "the words of the speakers, but the minds of the hearers."²⁴⁶ He said that the government may not be able to control what people say, but it could guarantee "everything worth saying shall be said."²⁴⁷ In other words, freedom of expression is valued chiefly for its essential contribution to deliberative democracy. Not only do other expressive values, such as facilitating individual autonomy,²⁴⁸ take a back seat to the self-governance value, but also they can be threats to it. To the extent that occurs, affirmative theorists argue that state actors are best equipped to address the threat. Indeed, even economics scholar Ronald Coase, the free-market champion and founder of the field of law and economics, believes "the case for government intervention in the market for ideas is much stronger than it is, in general, in the market for goods."²⁴⁹ Put differently, these theorists contend that media corporations have a duty to maintain a diverse and robust public discourse, and if they fail, government must force them to do so. Affirmative theorists, then, generally support state action to remedy threats to democratic participation from private power.

These perspectives should inform any theorizing about the values of, and controls over, freedom of expression in a networked society. Scholars in the field of "Cyberlaw" have debated whether the Internet is subject to the laws of the brick-and-mortar world since the Internet first went public.²⁵⁰ The consensus today is that such laws can and should apply to the Internet in certain situations, but the larger concern is how extralegal regulatory forms affect the Internet.²⁵¹ Legal scholar Lawrence Lessig famously argued that

²⁴⁶ *Id.* at 26.

²⁴⁷ *Id.* at 26.

²⁴⁸ See generally C. EDWIN BAKER, HUMAN LIBERTY AND FREEDOM OF SPEECH 48 (1989) (arguing that the fundamental principle of the First Amendment is to promote "individual self-fulfillment and participation in change, . . . self-realization and self-determination").

²⁴⁹ Ronald Coase, *The Market for Goods and the Market for Ideas*, 64 THE AM. ECON. REV. 384, 389 (1974).

²⁵⁰ See, e.g., GOLDSMITH AND WU, *supra* note 31; Lastowka, *supra* note 119; Andrea Braithwaite, 'Seriously, Get Out': *Feminists on the Forums and the War(craft) on Women*, 16 NEW MEDIA & SOC'Y 703 (2014).

²⁵¹ Ziewitz and Pentzold, *supra* note 48, at 312.

the Internet could be both liberating and constraining—and that social norms, the economic marketplace, and technological design all had greater power to regulate Internet activities than law.²⁵² Focusing on such “law-like effects”²⁵³ in the network “systematically treat[s] technical decision-making as a source of Internet policy that, in its effects if not its source, now interpenetrates legal policy-making to create the communicative and informational environment in which we live.”²⁵⁴

An example is Section 230 of the Communications Decency Act, which has increased the salience of the “law-like effects” of intermediaries’ ability to control user content.²⁵⁵ The statute states that digital intermediaries hosting third-party content shall not be treated as its publisher or speaker, and the statute grants the intermediaries immunity from civil liability if they voluntarily restrict access to the content, regardless of whether it is protected constitutionally.²⁵⁶ Section 230 was intended to foster online expressive activities, not stifle them by incentivizing intermediary control. However, having the capacity to choose whether to exercise control of user content without fear of liability is a powerful legal subsidy that digital intermediaries enjoy. Legal scholar Rebecca Tushnet, echoing the philosophy of Professors Barron²⁵⁷ and Sunstein,²⁵⁸ believes that Section 230 affords “dominant providers [both] substantial market control”²⁵⁹ and a “substantial concentration[] of power over public discourse.”²⁶⁰ She has argued that intermediaries “do not generally compete to protect user rights,”²⁶¹ and thus limiting intermediaries’ liability for user

²⁵² LESSIG, *supra* note 38.

²⁵³ Sandra Braman, *The Interpretation of Technical and Legal Decision-Making for the Internet*, 13 INFO., COMM. & SOC’Y 309, 309 (2010).

²⁵⁴ *Id.* at 311.

²⁵⁵ Nunziato, *supra* note 51.

²⁵⁶ 47 U.S.C. § 230 (2012).

²⁵⁷ Jerome A. Barron, *Access to the Press: A New First Amendment Right*, 80 HARV. L. REV. 1641 (1967).

²⁵⁸ SUNSTEIN, *supra* note 242.

²⁵⁹ Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 GEO. WASH. L. REV. 986, 994 (2008).

²⁶⁰ *Id.* at 993.

²⁶¹ *Id.* at 1004.

content should require a concomitant limiting of their capacity to control online expressive activities.²⁶²

Exactly how that capacity should be limited is the subject of great debate among Internet law scholars. One approach is to treat digital intermediaries as public forums.²⁶³ The theory is that the intermediaries perform services like those performed by public parks or squares, insofar as individuals use both environments to engage in expressive activities. The implication is that the intermediaries' speech regulation would be subject to First Amendment analysis. However, this approach has not always prevailed in court. In *Cyber Promotions Inc. v. America Online Inc.*,²⁶⁴ the United States District Court for the Eastern District of Pennsylvania held that AOL's email service was not the "functional equivalent" of a public forum.²⁶⁵ In other words, AOL was not acting as an agent supplying a forum for communication that state actors would normally make available. The court also held that AOL, unlike cable systems, did not control the "critical pathway" of communication.²⁶⁶ Rather, AOL was one of multiple pathways for publishing information online.

Some extol this ruling because, as legal scholar Eric Goldman put it, "[c]onverting private . . . providers into state actors could, paradoxically, limit speech rather than increase it."²⁶⁷ Others say the similarity of digital intermediaries and public forums should be embraced in the conventional sense and that the similarity should guide the formation of free-speech values vis-à-vis intermediaries. Professor Balkin believes the intermediaries are "'public' in the sense that their value as networks arises from public participation that produces network effects,"²⁶⁸ and he has argued that "digital technologies change the social conditions in which people speak,

²⁶² *Id.* at 1009.

²⁶³ See Sandra Braman & Stephanie Lynch, *Advantage ISP: Terms of Service as Media Law*, 5 *NEW MEDIA & SOC'Y* 422 (2003); Nunziato, *supra* note 51.

²⁶⁴ 948 F. Supp. 436 (E.D. Pa. 1996).

²⁶⁵ *Id.* at 443.

²⁶⁶ *Id.* at 453–55.

²⁶⁷ Eric Goldman, *Speech Showdowns at the Virtual Corral*, 21 *SANTA CLARA COMPUTER & HIGH TECH. L. J.* 845, 851 (2005).

²⁶⁸ Balkin, *supra* note 243, at 23.

... bring[ing] to light features of freedom of speech that have always existed in the background but now become foregrounded.”²⁶⁹ In that respect, the technologies advance the central purpose of freedom of speech—which is “to promote democratic culture” by affording individuals “a fair opportunity to participate in the forms of meaning making that constitute them as individuals.”²⁷⁰

B. Synthesis

At their core, affirmative theories of freedom of expression make two arguments. First, the most important expressive value is mass participation by individuals in a self-governing democracy. Second, that value faces threats not only from state actors but also from powerful private actors (e.g., large media conglomerates) that constrain individuals’ participation in the public discourse. Although some affirmative theorists take the extra step of proposing policies whereby state actors use public law to limit the private actors’ power, this article does not take that step. Rather, this article uses affirmative theories to present a framework for understanding the threats that digital intermediaries pose to the public discourse through content governance. Connecting the concepts from Internet governance with Professor Lessig’s theory of regulation helps bring the study of content governance into the ambit of both legal scholarship and First Amendment theory.

Professor Lessig has argued that speech regulations should be analyzed through the lens of key First Amendment values.²⁷¹ He proposed a model with four “modalities” of regulation: law, social norms, the marketplace, and the design of technologies facilitating the activity being regulated.²⁷² Law regulates an activity by punishing it or by codifying incentives that encourage individuals to engage in alternative activities. Norms, often defined by a society’s moral values, regulate an activity by socially stigmatizing or encouraging it. Markets regulate an activity by making it costly

²⁶⁹ *Id.* at 2.

²⁷⁰ *Id.* at 3.

²⁷¹ Lessig, *supra* note 38.

²⁷² *Id.* at 124.

or by incentivizing individuals to engage in alternative activities. And, finally, the design (“architecture”) of a technology facilitating an activity regulates it by enabling it to be performed only in the way permitted by the technology.²⁷³ Importantly, all of these modalities are interdependent.²⁷⁴ They interact with one another in the context of content governance.

First, consider law. Section 230²⁷⁵ grants commercial intermediaries immunity from tort liability for third-party content. Not only are intermediaries immune from liability for hosting the content on their platforms, they are also immune from liability for removing it—essentially, from assuming control of it. Thus, Section 230 encourages content governance by promising that intermediaries will not be punished for it. Meanwhile, case law indicates that commercial intermediaries have a First Amendment right to manage content on their platforms.²⁷⁶

Second, consider norms. This modality is the most important to this article. Because law grants intermediaries so much discretion to manage user content, the intermediaries must devise and enact

²⁷³ Lessig gives the example of smoking to illustrate his four-part model. Laws can make it more difficult to smoke in public places, thereby leading people to consider quitting. Social stigmatization may lead people to quit, lest they become social pariahs. The high cost of cigarettes may make the opportunity cost of smoking too high for many people, leading them to quit. Finally, the design of a cigarette makes smoking odorous and leads to lung cancer. If one wants to smoke but does not want to smell or get lung cancer, one must choose not to smoke or to use an alternative to smoking (e.g., an e-cigarette). *Id.* at 122–23.

²⁷⁴ Continuing the smoking example, the high cost of cigarettes is often the result of laws that set the taxes governments collect on the product. The fact that cigarettes have a strong smell may lead to smoking being a socially stigmatized activity, which may in turn lead to laws that ban the activity in public places.

²⁷⁵ 47 U.S.C. § 230 (2012).

²⁷⁶ See also *Miami Herald Pub. Co. v. Tornillo*, 418 U.S. 241 (1974) (holding that a Florida statute requiring newspapers to publish responses from individuals who believed they were attacked in newspapers amounted to an unconstitutional prior restraint); *Cyber Promotions v. AOL*, 948 F. Supp. 436 (E.D. Pa. 1996) (holding that AOL’s email service did not amount to a “critical pathway” of communication, and thus the government could not regulate it); see generally Bruce W. Sanford & Jane E. Kirtley, *The First Amendment Tradition and Its Critics*, in *THE PRESS* 263 (Geneva Overholser & Kathleen Hall Jamieson eds., 2005).

their own policies to do so. Content-governance norms are constructed through a process of negotiation.²⁷⁷ Sometimes, employees of digital intermediaries decide which types of content will be subject to private governance, and other times individual users define what constitutes undesirable content by pressuring intermediaries to adopt certain community values.²⁷⁸

Third, consider the market. As discussed above, the networked economy's structure incentivizes intermediaries to make their platforms a welcome place and experience for users.²⁷⁹ The goal is to attract and retain as many users as possible. This modality, then, is connected to the norm modality: what sells will be what the user community deems desirable. So, if community norms dictate that certain speech does not sell (i.e., its presence deters individuals from using a platform), that speech is not likely to survive because of market pressure.

Finally, consider design. Whatever norms commercial intermediaries follow to govern content, they will be baked into the platforms' design (which, in this context, Lessig refers to as "code"). For example, platforms may give users the ability to flag offensive content (i.e., to notify the intermediary about the content and request that some action be taken).²⁸⁰ The act of removing content, or of effectively excommunicating the individual who created it, is a function of platform design.

Again, the modalities are interdependent, showing, among other things, that technological design must be conceived as a product of social norms. Technology policy "is the construction and [the] legal authorization of sociotechnical systems designed to select out those activities we want to render impossible (and the converse, those we hope to encourage)."²⁸¹ "[T]echnologies are the product of political choices and have political consequences that must be recognized and acknowledged."²⁸² Political choices and

²⁷⁷ See generally Langlois, *supra* note 62.

²⁷⁸ See generally Crawford & Gillespie, *supra* note 106.

²⁷⁹ van Dijck, *supra* note 31, at 51.

²⁸⁰ See generally Crawford & Gillespie, *supra* note 106.

²⁸¹ GILLESPIE, *supra* note 41, at 10.

²⁸² *Id.* at 66.

consequences imply an inherent conflict in technological design and implementation. We build technologies in both the physical and the “rhetorical sense, drawing linguistic boundaries around them to indicate what is part of the [technology] and what is not, shaping how the relationship between elements can and will be characterized.”²⁸³ In short, rhetoric and technology go hand-in-hand because technology is, itself, an argument and an interpretation of how it should be used.

V. CONCLUSION

Recall that Professor Rosen said the task of translating democratic principles for our time and technologies falls not only to judges but also to regulators, legislators, and technologists.²⁸⁴ And Professor Balkin said as our “lives are increasingly dominated by information technology and information flows,” the doctrinal First Amendment, with its focus on rights against the government, will grow “increasingly irrelevant” to the future’s key free speech battles.²⁸⁵ Indeed, policy discussions worldwide are converging on the idea that “the private sector has a shared responsibility to help safeguard free expression,”²⁸⁶ and this article advances those discussions and makes a significant contribution to the related scholarly literature by synthesizing Internet governance concepts and theories with those of content management and normative theories regarding the social value and limits of freedom of expression. This article also puts in concrete terms, by evaluating the chain of digital intermediaries that make up the Internet’s basic infrastructure, the proposition that intermediaries are regularly conducting “private . . . speech regulation.”²⁸⁷

Interestingly, new realist scholars once saw broadcast media as a threat to individual participation in the public discourse. Professor Barron argued, in fact, that U.S. broadcasters wielded

²⁸³ *Id.* at 75.

²⁸⁴ Jeffrey Rosen, “The Deciders: Facebook, Google, and the Future of Privacy and Free Speech,” *in* CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE 81 (Jeffrey Rosen & Benjamin Wittes, eds., 2011).

²⁸⁵ Balkin, *supra* note 83, at 427.

²⁸⁶ Clinton, *supra* note 17.

²⁸⁷ Benesch & MacKinnon, *supra* note 10.

enormous power over the public discourse simply by exercising their First Amendment rights to manage their own programming.²⁸⁸ He said the resulting power imbalance—between broadcasters and viewers—derived from the medium’s pervasiveness, the broadcasters’ ability to reach large national audiences, and the reality that the limited number of broadcasting channels was concentrated in the hands of a few large corporations.²⁸⁹ Famously, Barron contended that broadcasters’ power was so great that American courts should recognize a First Amendment right of access—for individuals—to the broadcasters’ otherwise closed channels of communication, lest the public discourse grow stagnant.²⁹⁰

Internet communications were seen as the antidote to that power imbalance,²⁹¹ because individuals would have greater ability to communicate messages that compete with those of large media companies. More than a decade before the Web’s invention, sociologist and technologist Ithiel de Sola Pool recognized the potential of electronic communication to be an “expander[] of human culture”²⁹² that would end the monopolistic reign of large broadcast corporations.²⁹³ Networked communication has not exactly realized that potential. The Internet, like broadcast, is a medium in which a few major players dominate traffic and crowd out alternative perspectives.²⁹⁴ For scholars like Pool and Barron, the issues presented by content governance are a step back to the days of corporate power over the public discourse through control of broadcast media. The main question that remains is how far backward this step is. Answering that question is a task of future research.

In the meantime, we urge intermediaries to be transparent regarding their content-governance practices. They are already

²⁸⁸ Barron, *supra* note 257.

²⁸⁹ *Id.*

²⁹⁰ *Id.*

²⁹¹ *See generally* ITHIEL DE SOLA POOL, TECHNOLOGIES OF FREEDOM: ON FREE SPEECH IN AN ELECTRONIC AGE (1983); Barron, *supra* note 257.

²⁹² POOL, *supra* note 291, at 226.

²⁹³ *Id.* at 246–47.

²⁹⁴ Barron, *supra* note 257, at 1644.

transparent in some ways—many have published their content rules and community standards, as well as reports about their interactions with government entities. However, they are not always transparent in applying their rules and standards, leaving users and others to wonder—in too many cases—how or why a particular decision was made. Intermediaries must be as open as possible to maintain the robustness of the public discourse they facilitate. Their actions merit scrutiny. After all, the phenomenon of intermediaries may not be new, but the Internet’s extensive reliance on them, combined with the public’s extensive use of the Internet, has amplified significantly the influence and importance of digital intermediaries to the public discourse.²⁹⁵ They are major players in the evolving story of free expression.

²⁹⁵ Ardia, *supra* note 20, at 378.