Bourdieu, P. (1986). The forms of capital (R. Nice, Trans.). In J.G. Richardson (Ed.), Handbook of theory and research for the sociology of education. New York: Greenwood Press.
Bousquet, M., & Willa, K. (Eds.). (2003). The politics of information: The electronic mediation of social change. Boulder, CO: Alt X Press.
Brooks, F. (1995). The mythical man-month. Boston, MA: Addison-Wesley. (Original work published 1975)
Hofstede, G. (1980). Culture's consequences: International differences in work-related values. Beverly Hills, CA: Sage.
Raymond, E. (1988, March). The cathedral and the bazaar. First Monday, 3(3).

Deborah E. Swain
School of Library and Information Sciences
North Carolina Central University
James E. Shepard Library
Durham, NC 27707
E-mail: dswain@nccu.edu

Published online 2 May 2011 in Wiley Online Library (wileyonlinelibrary.com).
DOI: 10.1002/asi.21548

Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace. Edited by Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski, and Jonathan Zittrain. Cambridge, MA: MIT Press, 2010. 656 pp. $25.00 (ISBN-10: 0-262-51435-4)

Networks and States: The Global Politics of Internet Governance. Milton L. Mueller. Cambridge, MA: MIT Press, 2010. 280 pp. $35.00 (ISBN-10: 0-262-01459-9)

A recent series of events—Google's dispute with China, Secretary of State Hillary Clinton's speech on Internet freedom, the Egyptian government shutting off nearly all Internet services during the 2011 pro-democracy revolution, .xxx domain approval by ICANN after much political controversy—is indicative of the heightening global politics surrounding the Internet.

Two books—*Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace,* edited by Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski, and Jonathan Zittrain, and *Networks and States: The Global Politics of Internet Governance,* by Milton L. Mueller—have drawn attention and provide context to exactly these global political struggles to govern the world's distributed communication infrastructure, increase governments' efforts to control, and reassert sovereignty rights over cyberspace by nation states. Both books contribute to explicating the complex tensions between nation states and the extraterritorial nature of the Internet.

Access Controlled centers around new trends of Internet censorship and surveillance mechanisms that are deployed by governments, private sectors, civil societies, and individuals; *Networks and States* treats a broader subject matter: the global network governance that encompasses censorship and surveillance, dealing with the fundamental question of how the Internet should be governed given its transnational nature and seeking an alternative model of Internet governance.

Deibert et al. highlight both states and private actors and their relationships in shaping censorship and surveillance; Mueller's work specifically problematizes the role of nation states in cyberspace. If one has not yet been convinced that the Internet is far from value neutral, once again these books corroborate and stress the fact that cyberspace has grown ever more tightly intertwined with global political economy and has become a site of political, economic, and cultural struggle among nation states.

Access Controlled is the sequel to *Access Denied: The Practice and Policy of Global Internet Filtering* published in 2008 by the OpenNet Initiative (ONI)—a collaboration between the Citizen Lab at the University of Toronto's Munk Centre for International Studies, Harvard's Berkman Center for Internet and Society, and the SecDev Group. The change in the title from "denied" to "controlled" suggests that this volume elucidates the shift in censorship methods from denying access to controlling access through various means in cyberspace (p. 6). This updated ONI project moves beyond the traditional government censorship framework and consider multidimensional aspects of censorship and surveillance practices that are entangled with a variety of actors. The book comprises two parts. The first part is a collection of writings that capture the essence of new trends of global Internet censorship and surveillance: the second part is focused on the analysis of the ONI survey of 65 countries on censorship and surveillance mechanisms.

In the first two chapters, Deibert and Rohozinski broadly define three generations of Internet controls. The first generation refers to the so-called "Chinese style" filtering techniques that simply deny access to server domains, keywords, specific Internet resources, IP addresses, etc. (p. 22). Second-generation controls deploy legal and normative environments such as doctrines of information security and defamation and create "technical capabilities that enable actors to deny access to information resources 'just in time'" (p. 24). Third-generation controls are more sophisticated and multidimensional. Deibert and Rohozinski describe it this way: "The focus is less on denying access than successfully competing with potential threats through effective counter information campaigns that overwhelm, discredit, or demoralize opponents" (p. 7). An example of a third-generation control is the recent revelation by the *Guardian* that the U.S. military is developing so-called "sock puppet" software to manipulate social media sites secretly (Jarvis, 2011).

Deibert and Rohozinski discovered that the Commonwealth of Independent States (CIS) are driving the second and third generation of controls by encompassing extensive means of legal, regulatory mechanisms, such as registration requirements for websites, restrictions of content under "public order" and "illegal" or "inappropriate" content, as well as technical tactics like distributed denial of service attacks. One of the reasons behind shifting control strategies by the CIS is that state actors recognize the Internet's potential for mobilizing political opposition beyond use of websites and blogs (p. 16).

Chapter 3, by Roberts and Palfrey, is valuable to anyone who is interested in information policy. It offers a comprehensive technical landscape for readers, explaining where, how, and by whom surveillance takes place within the Internet architecture, and it challenges common perceptions that distributed Internet architecture makes it impossible to censor networks comprehensively. Roberts and Palfrey divide surveillance into three categories—networks, servers, and clients—and demonstrate how data are vulnerable to exposure when traveling between these locations at any given time. Roberts and Palfrey say that the "Internet is a 'surveillance-ready' technology. There is a wide range of choices for any state that wishes to know more about its citizens" (p. 34).

Whereas Roberts and Palfrey discuss state-led censorship measures, in chapter 5, Zuckerman reveals self-regulated censorship by Internet intermediaries like online service providers (OSPs). Zuckerman reports a few cases of OSPs that have voluntarily censored web content to comply—as it turns out, based on misinterpretation of U.S. law—with the U.S. Treasury Department's restriction and export controls set by the Office of Foreign Assets Control (OFAC). For example, in 2009, BlueHost, an American web-hosting company, disabled a Zimbabwean human rights organization's website, LinkedIn.com blocked Syrian users, and Microsoft turned off Live Message Service in Iran, Syria, Sudan, Cuba, and North Korea citing OFAC sanctions (p. 81). Zuckerman states that the logic behind these OSP's self-regulated censorship is to avoid business risk or burden of legal and other costs of hosting potentially controversial content. Zuckerman's cases raise the question of relinquishing state regulatory power over to private actors because private actors tend to value their "bottom line" over the principle of freedom of expression.

The contribution of the first part of *Access Controlled* reveals new emerging censorship trends around the globe and how extensive surveillance of Internet traffic is possible through tapping into choke points within the wider Internet infrastructure. However, and more importantly,

ONI researchers present various actors that are involved in monitoring Internet traffic, from governments, states, or privately owned ISPs and OSPs to search engines to market research companies, like Comscore, to client-side antivirus software; the book and places surveillance within concrete technical, legal, social and political contexts. The research of censorship and surveillance often focuses only on the role of states, yet ONI researchers address not only the role of states but also on how current political economy changes the nature of censorship.

As private actors play increasingly significant roles, one needs to ask whether censorship and, in particular, surveillance practices by the private sector can be conceptualized within a traditional censorship framework. ONI research shows that companies like Google, Comscore and Facebook deploy various means of surveillance practices to achieve competitive advantage. For these companies, data are the assets and raw materials that can be invested, commodified, and recommodified; thus, collecting personal data by surveilling is part of their business practices. Given this, would it be possible to theorize current censorship and surveillance practices without a systematic critique of current capitalism that is centered around information?

The second part of *Access Controlled* provides a comprehensive country profile, including legal and regulatory frameworks, and demonstrates how second-generation and third-generation controls can be found within authoritarian states and increasingly deployed by advanced democratic states. The ONI survey demonstrates that although first-generation controls are still deployed by some countries, second-generation and third-generation mechanisms have become the dominant normative practices. According to ONI research, in regards to surveillance, the United States is considered "the most aggressive country in the world in terms of listening to online conversations" (p. 381). The results of the survey show the growing militarization of cyberspace by states and third-party actors around the world.

Mueller picks up on the fact that nation states are increasingly implementing national policies to control the Internet and asserting territorial boundaries in cyberspace. Mueller, a professor at the Syracuse University School of Information Studies, a leading Internet policy scholar and critical voice for U.S. unilateralism over the Internet Corporation for Assigned Names and Numbers (ICANN).

In *Networks and States*, Mueller laments the reterritorialization of cyberspace and argues that the role of states over global Internet politics has to be reduced; he says: "Nation states—including the United States of America, not just undemocratic ones—constitute some of the biggest threats to the global character and freedom of networked communication" (p. 253). Mueller takes the opposite position to Jack Goldsmith and Tim Wu, who recognize national sovereignty power over cyberspace in *Who Controls the Internet? Illusions of a Borderless World* (2006).

Mueller begins by presenting five unique ways that the Internet pressures nation states: (a) transnational scope of communication, which cuts across national jurisdictions; (b) boundless scale, a massive capacity for information generation, transmission, duplication, and storage; (c) distributed control via decentralized Internet protocols and distributed participation over networking; (d) the emergence of new institutions that are developing alongside the Internet such as ICANN and Internet Engineering Task Force (IEFT); and (e) changes in polity as collective action capabilities grow beyond the traditional nation state. One of Mueller's basic arguments is that because of the distinctiveness of the Internet, there is a need for a new form of Internet governance (pp. 4–5).

What are the possible new forms of governance? To explore answers to this question, Mueller delves into theories of network analysis such as analytical technique and networks as organizational forms in social science. In particular, he concentrates on concepts of network as organization from a variety of literature, including political science, economics, and sociology, and identifies new forms of governance such as networked governance, commons-based peer production, and multistakeholder governance.

In chapter 4, Mueller analyzes international institutional changes in Internet governance based on the conceptual foundations of network analysis and network as a form of governance by deconstructing a range of actors and forces that were involved in the United Nations (UN) World Summit on the Information Society (WSIS), held in Geneva, Switzerland (2003) and Tunis, Tunisia (2005). Mueller meticulously dissects WSIS processes and provides context of historical institutional development of Internet governance. He describes the politics of WSIS as representing "a clash between two models of global governance: one based on agreements among sovereign, territorial states; the other based on private contracting among transnational nonstate actors, but relying in some respects on the global hegemony of a single state" (p. 55).

Mueller succinctly articulates four controversies surrounding ICANN, which was one of the main focal points among nation states during WSIS. First, ICANN controls Internet names and addresses that play a critical function for routing information across the Internet; Second, ICANN controls the root server system that is required to coordinate and ensure connectivity across the Internet. Third, ICANN represents the privatization of what should be considered the global common resource of the Internet. Fourth, and most important, ICANN is controlled by the United States and represents global U.S. unilateralism (pp. 61–62).

ICANN is one central organization within a distributed communication infrastructure. Mueller points out that the WSIS process gave "national governments, international organizations, certain developing countries, and Europe an opportunity to openly challenge the legitimacy of the institutional innovation that was ICANN" (p. 60). He states that "WSIS inaugurated an explicit debate over the role of the nation-state in Internet governance. Governments, both democratic and undemocratic, felt the need to assert their belief that they should have authority over Internet-related public policy issues" (p. 60). Countries like Brazil argued that "the Internet is a public resource that should be managed by national governments and at an international level, by an intergovernmental body such as the ITU [International Telecommunications Union]" (p. 64).

During this period, according to Mueller, multilateral governance was incorporated within the discourse of Internet governance. The WSIS process challenged U.S. unilateralism, brought changes in ICANN, and led to the creation of Internet Governance Forum (IGF), which is based on the concept of multistakeholderism. Mueller concludes: "Broader, more public and contentious global dialogue fostered by the WSIS process started to loosen up those discursive and institutional boundaries" (p. 79). One of the significant results of the WSIS process that Mueller points out is "the implementation of the multistakeholder model of governance within the UN system" (p. 105). Although Mueller recognizes the importance of this change, he points out the limitation of multistakeholderism:

> [It] maintains the pretense that nation-states are stakeholders on an equal status with others. But given prevailing institutions as power relations, this is a dangerous fiction. States, especially great powers, can pick and choose when to engage in a way that the other groups cannot. (pp. 265–266)

Mueller devotes chapter 5 exclusively to documenting the role of nonstate actors, showing how WSIS became a mobilizing structure for transnational civil society groups, which, in turn, he calls the "new transnational policy network." Although many countries reasserted sovereign nations' right to determine "public policy" for the Internet (p. 80), Mueller suggests that WSIS also provided an opportunity to nonstate actors, which fostered the democratization and opening up of International organizations and extended the scope of Internet governance beyond ICT infrastructure to include equity and human rights related to Information and communication policy. A number of smaller issue networks converged to create a more stable transnational policy network, centered around the core network of advocacy groups such as the Campaign for Communication Rights in the Information Society (p. 88). Mueller states:

> WSIS brought together preexisting but fragmented advocacy networks around communication information policy and established stronger interpersonal and organizational relationships among transnational civil society actors in this policy domain. WSIS put a new transnational policy network on the map. (pp. 94–95)

DOI: 10.1002/asi

In a sophisticated way, Mueller analyzes and visualizes how various civil society advocates link together and create hubs of connection. His network analysis allows the reader to see how advocacy groups from developing countries are linked to part of the transnational policy network, but it also reveals unequal participation among players in civil society. On the one hand, this new transnational policy network represents inclusion through the web of networks, but on the other hand, it indirectly shows exclusion, which raises theoretical challenges to addressing unequal and uneven participation of civil society.

In chapters 7 through 10, Mueller describes the four crucial main drivers of Internet governance that generate transnational politics: intellectual property (IP), cyber-security, content regulation, and the control of critical Internet resources (Internet standards, domain names, IP addresses, and the interconnection and routing arrangements among ISPs). Mueller contextualizes how these four issues produce the ongoing debates and tension between traditional national state-based regulatory regimes and the Internet and force the generation of transnational public policy. Mueller introduces the term "organically developed internet institutions" (ODii), which have developed alongside the Internet and he considers them independent from traditional state-based institutions. ODii include groups that control critical resources like the Internet Engineering Task Force, The Internet Society, Regional Internet Registries (RIRs), and ICANN. Mueller states that ODii represent changes in Internet policy and governance from state actors to nonstate actors to more open and participatory processes while addressing ICANN's lack of accountability.

The last chapter encompasses one of Mueller's goals for this book: to advocate a new form of governance centered around his vision of cyberlibertarianism, which refers to "denationalized liberalism" or "networked liberalism." Mueller states that "cyber-libertarianism is not dead; it was never really born. It was more a prophetic vision than an ideology or 'ism' with a political and institutional program" (p. 268). He presents a political spectrum and offers quadrants to explicate Internet policy. The axes are Transnational/National and Networking/Hierarchy; the quadrants are Denationalized Liberalism, Networked Nationalism, Global Governmentality, and Cyber-Reactionaries (p. 256). In the end, Mueller promotes "denationalized liberalism" to reconcile between nation states and the global Internet. He concludes:

> Denationalized liberalism embraces both property and commons and seeks to leverage their complementarities. It recognizes the coexistence and interdependence of markets, exclusive property rights, and shared/unowned resources in communication and information. It rejects the false idea that commons and property are mutually exclusive, totalizing principles for economic organization, seeing them instead as distinctive methods of organizing access to resources with their own virtues and failings. (p. 270)

Mueller is not the first person to claim the possibility of coexistence of property and commons in harmonious ways; but this argument undermines the expansionist logic of capitalism that spurs the enclosure movement. In fact, enclosure is part and parcel of the accumulation strategies of capitalism; under the current neoliberal policy that Mueller embraces, privatization of the commons has been exponentially accelerated.

Although Mueller states that "the Internet itself embodies an unusually successful example of this complementary relationship between private sectors and commons" (p. 270), the Internet shows, in fact, how a commons can be taken over by global capital with state assistance and turned into a new site of profit making for transnational corporations. Mueller considers nonstate actors like ICANN as an alternative form of governance, but, in reality, ICANN was an institution that facilitated the privatization of the Internet commons. Mueller correctly underscores the critical question—how should the Internet be governed?—but additional questions need to be asked including: How can the Internet be turned into a true global commons like air and water? What kind of governance is required to achieve it?

Throughout the book, Mueller consistently problematizes the assertion of state power over cyberspace and proposes a denationalized liberalism; but to a lesser extent, he emphasizes the role of transnational corporations (TNCs), which dominate current global political economy. As nonstate actors, TNCs aligning with governments (sometimes de-aligning) have influenced the policy areas that Mueller identifies as the four drivers of Internet governance. Because Mueller calls into question the nation state as the principal institution of Internet governance, one might also question the private sector as the principal institution as well. If the vision of governance has to be denationalized or "sovereignty free," then might it also need to be "de-corporatized" or "corporation-free?"

Mueller provides an amazingly detailed, updated, and in-depth overview of the political debates and issues surrounding current Internet governance. Regardless of whether one shares his vision of denationalized liberalism, the book offers important insights on Internet governance and information policy. Both *Networks and States* and *Access Controlled* thoroughly treat a wide range of Internet policy issues and are timely scholarly pieces as the coming political and economic struggles over cyberspace only intensify.

References

Goldsmith, J.L., & Wu, T. (2006). Who controls the Internet?: Illusions of a borderless world. New York: Oxford University Press.

Jarvis, J. (2011). America's absurd stab at systematising sock puppetry. Guardian. Retrieved from http://www.guardian.co.uk/commentisfree/cifamerica/2011/mar/17/us- internet-morals-clumsy-spammer

ShinJoung Yeo
544 Guerrero Street #2
San Francisco CA 94110
E-mail: yeo1@illinois.edu

Published online 9 May 2011 in Wiley Online Library (wileyonlinelibrary.com).
DOI: 10.1002/asi.21554

Alternative and Activist New Media. Leah A. Lievrouw. New York: Wiley, 2011. 294 pp. $19.95 (paper) (ISBN 9780745641843).

In *Alternative and Activist New Media*, Leah Lievrouw offers a comprehensive introduction to new media activism that will find a ready audience among readers new to studies of online activism. Noting the ongoing shift away from the dominance of so-called mainstream media to other genres and modes of communication, Lievrouw aims in this book to offer a framework for thinking about new media: How "new" are new media? What are they for? Who gets to use them? Lievrouw engages these questions by looking at five genres of new media that are explicitly alternative and/or activist. That is, they are ways of using media that contest its traditional usage and push for different kinds of engagement, authorship, and participation as well as for social, political, and/or cultural change. Through these examples at the margins, Lievrouw informs our broader understanding of media and communication in the Internet age.

The book has a secondary aim as well: to offer support for using the concept of mediation in theoretical understandings of contemporary media. In Lievrouw's account, the mediation perspective emphasizes what people *do* with media, attending specifically to how they adapt and modify existing technologies and blur the line between producer and consumer (or user) to render media consumption interactive. Lievrouw contends that her summary of alternative and activist new media lends support for a mediation perspective in communication theory. It is important to note, however, that this theoretical aim is decidedly secondary to the overall descriptive purpose of the book, making this book a particularly useful starting point for readers with an interest in digital media studies who are unfamiliar with current debates in communication