

Four Phases of Internet Regulation

Forthcoming in *Social Research*, Vol. 77, No. 3 (Fall, 2010)

John Palfrey[†]
Harvard Law School
1545 Massachusetts Avenue
Cambridge, MA 02138

Abstract:

The four phases of Internet regulation are the “open Internet” period, from the network’s formation through about 2000; “access denied,” through about 2005; “access controlled,” through the present day (2010); and “access contested,” the phase into which we are entering.

[†] John Palfrey is a professor of law at Harvard Law School and a faculty co-director of the Berkman Center for Internet & Society at Harvard University. This article draws upon research and arguments developed by members of the OpenNet Initiative, which is a collaboration that joins researchers at the Citizen Lab at the Munk Centre, University of Toronto (Prof. Ron Deibert, principal investigator), the SecDev Group (where Rafal Rohozinski is principal investigator), and the Berkman Center (where the author and Prof. Jonathan Zittrain are co-principal investigators). The author is grateful to Rob Faris, Jill York, and the large number of researchers who have participated in gathering, over nearly a decade, the data on which this article draws. Any errors or omissions are the author’s alone.

In this article, I describe the role of technology and its use in limiting access to knowledge during four phases of development of the Internet. The possibilities associated with how people are using technology to strengthen democracies around the world make up an equally important part of the story. The four phases of Internet regulation are the “open Internet” period, from the network’s birth through about 2000; “access denied,” through about 2005; “access controlled,” through the present day (2010); and “access contested,” the phase into which we are entering.

Phase 1: The Open Internet (the 1960s to 2000).

The first phase, roughly from the Internet’s initial formation in the 1960s through about 2000, is the period of the “open Internet.” This term was intended to convey descriptive, predictive, and normative meanings. During this initial period of the network’s development, the dominant theory – to the extent that anyone was thinking seriously about regulation at all – was that the Internet itself was a separate space, often called “cyberspace.” The concept of cyberspace melded the creativity of the science fiction writer with the aspirations of the democratic theorist dreaming of a fresh start. As a descriptive matter, there was much truth to the argument: up until the late 1990s, most states tended either to ignore online activities or to regulate them very lightly. When states did pay attention to activities online, they tended to think about and treat them very differently from activities in real-space. The term proved inaccurate as a predictive matter. On a normative level, there is still salience to the concept of the open net that is worth continuing to bear in mind.

Though the era of the “open Internet”, as a descriptive matter, is long past, there are important elements of the theory behind it that persist to the present day. There is truth to the argument, for instance, that the Internet allows us to hear more speech from more people than ever before. To this extent, the Internet can allow greater freedoms than humans previously enjoyed, especially in closed regimes where the state controls the mouthpieces to which citizens listen. Governments can use the same technologies to become more open and more transparent in their operations. This theory is at the core of the openness initiatives championed and implemented by the Obama Administration (Noveck 2008). Cross-cultural understanding could flourish as never before, now that these digital networks connect people from all around the world in new and important ways at very low cost. Communications across diaspora populations can thrive in meaningful ways.

Just as we think about how states have responded to the growth of the Internet and its usage, it is crucial to see the story also from the perspective of the individual and of the groups that they form, mediated by these technologies. The individual has greater autonomy in a networked public sphere. (Benkler 2005) One can access more information than ever before in human history at little cost. With the Internet, we can – over time – come to have an online, digital Library of Alexandria, a place online where a massive amount of the world’s knowledge can be stored and accessed from anywhere on the planet. An individual in nearly any country on earth, assuming they have an Internet

connection, can already access a vast store of information, much greater than what anyone a century ago could have imagined.

The great power of the Internet as a force for democratization is in collective action. The amplifying effect of Internet technologies and of digital media can also be seen in group formation and power. The Internet can serve as a facilitator of the formation of online groups, which in turn will have an impact on democracy and governance. There is enormous power in this notion of quickly forming and dissolving groups in the form of flash mobs. (Rheingold 2003) An example from the 2008 election cycle in the United States is the extent to which supporters of a candidate like Ron Paul, who was not a mainstream candidate, are able to use the technology to identify and connect with like-minded activists and voters. Individuals are able to use these cheap technologies as organizing tools to pull others around them together and, through collective action, have a greater effect on a political process than they might have had absent their ability to use these technologies.

There are many other examples of this phenomenon around the world, in which fringe candidates or groups are able to fight above their weight when they combine online activities with offline activism. This story globally is a lot clearer than in the United States. One can observe a broad range of examples through Global Voices, an online community of activists and citizen journalists. (Global Voices 2010) These examples show the power of networked digital technologies in terms of greater access of

knowledge and proliferation that are the partial expression of these first-generation theories about the power and promise of an open net.

Another way to see the changes in democratic discourse in a networked world is to look closely at the conversations happening in the world's blogospheres. Through this lens, we can examine today the ways in which people of various cultures create environments in which they are talking to one another in a virtual space, joined by a common language. It is increasingly possible to map the conversations happening in public online to understand better what is happening in this discourse and how people are relating to one another, to information, and to institutions through digital media. Through these research methods, we can gain new insights into how discourse in these online environments might affect the politics of culture and dissent. (Kelly et al. 2008; Etling et al. 2009)

A lens into what is happening online is the expression in the Egyptian blogosphere. Egypt is a state often thought of as having a fair amount of control over media. There is a robust political discussion going on online in Egypt, in which people are talking about Islam, politics, foreign affairs, and so forth. There are powerful forms of discourse that we can illuminate using social science measures that prove that there is a growth in using these technologies; that individuals can have more voice by using these tools as amplifiers and as connectors; and that there are culturally and politically important conversations going on in the networked public sphere.

Any careful examination of a blogosphere will demonstrate, too, that there are also problems associated with what people do in these spaces. This is true whether the context is the United States or Myanmar. There are sound reasons for any state to seek to restrict online speech and to practice increased surveillance, from child protection to routine law enforcement, with which few would argue.

Terrorism is among the chief justifications for limitation of speech online and otherwise throughout societies. Other articles in this issue of *Social Research* make plain the challenges associated with this issue. While we celebrate the ways in which information and communications technologies, whether digital or not, are useful to those who would bring democracy about around the world, it is equally important to realize that the very same tools can be useful to those who would harm other people. These are neutral technologies, useful for the activist, useful for the state, and useful for the terrorist.

We ought to see information and communications technologies as connected to the rest of life in virtually every respect. One of the primary reasons for Internet regulation is child safety and access to pornography, not new concerns but topics that are of universal interest to parents, teachers, and policy-makers around the world. Nearly all of the problems that arise in offline space find their way into the online environment, and in turn give rise to control strategies.

Cycle back to the theory of the open net and its merits and demerits. The descriptive and some of the normative elements of the original “open net” theories were not only

accurate, but remain helpful and important to this day. The parts of the “open net” theories that were wrong were those that asserted a certain “nature” in the net that would persist over time. (Barlow 1996) In this strong form of the “open net” argument, the emphasis was descriptive in nature but rather predictive. The argument, at its core, was that the Internet represented a separate environment from real-space that had qualities that made it hard, or impossible, to regulate. The notion was that cyberspace stood apart from geographic boundaries. Though the rhetoric of the open Internet was (and remains, in some respects) compelling, it was wrong as a predictive matter. It was wrong in large measure because nothing in the technology is unrelated to human behavior. We have simply been wrapping our lives into this hybrid reality, one that is both virtual and analog – all of it “real” – at the same time. All of the actions we are taking using these technologies, whether on a virtual platform or on a real platform, are effectively interconnected and could be regulated. In turn, our activities online have been regulated, and in a range of ways that have changed over time.

Phase 2: Access Denied (2000 to 2005).

The second phase of development of the Internet, from roughly 2000 to 2005, is the “Access Denied” period. During this second era, states and others came to think of activities and expression on the Internet as things that needed to be blocked or managed in various ways. The thinking was that certain acts of speech and organizing online needed to be regulated like any other. The initial reaction, by states such as China and

Saudi Arabia in the first instance, was to erect filters or other means to block people from accessing certain information.

The world may appear borderless from when seen from cyberspace, but geopolitical lines are in fact well-established online. The fact that extensive Internet filtering occurs at a national level around the world is clearly documented. (Deibert et al. 2008 and 2010) Through a collaborative research effort called the OpenNet Initiative, the Citizen Lab at the University of Toronto, the Berkman Center for Internet and Society at Harvard University, and the SecDev Group have together compared the Internet filtering practices of a series of states in a systematic, methodologically rigorous fashion over the past eight years. (OpenNet Initiative 2010) We have sought to reach substantive conclusions about the nature and extent of Internet filtering in 70 states and over 289 Internet service providers. We initially focused much of our research on states in the Middle East and North Africa, Asia, and Central Asia, where the world's most extensive filtering takes place. Our research has also come to cover states in every region of the world, including North America and Western Europe, where forms of speech regulation other than technical Internet filtering at the state level are the norm. Through an advanced series of methodologies, we have tested well over 100,000 web sites for accessibility over the past eight years and recorded the results in a consolidated database, from which we are able to draw broad conclusions about Internet censorship practices around the world and over time.

Filtering implementations (and their respective scopes and levels of effectiveness) vary widely among the countries we have studied. China continues to institute by far the most intricate filtering regime in the world, with blocking occurring at multiple levels of the network and covering content that spans a wide range of topic areas. Though its filtering program is widely discussed, Singapore, by contrast, blocks access to only a handful of sites, each pornographic in nature. Most other states that we are studying implement filtering regimes that fall between the poles of China and Singapore, each with significant variation from one to the next. These filtering regimes are properly understood only in the political, legal, religious and social context in which they arise.

Internet filtering occurs in different ways in different parts of the world. Some states implement a software application developed by one of a small handful of United States-based technology providers. Burma, in the first incarnation of its filtering regime, used an open source product for filtering, called DansGuardian. Others rely less heavily on technology solutions and more extensively on “soft controls.” Sometimes the filtering regime is supported explicitly by the state’s legal code; in other cases, the filtering regime is carried out through a national security authority. In yet other instances, the regulation is simply presumed to be permissible. The content blocked spans a wide range of social, religious, and political information. Our studies have combined a review of whether individual citizens could access sites in a “global basket” of bellwether sites to test in every jurisdiction across a variety of sensitive areas – akin to a stock index sorted by sector—as well as a list of Web sites likely to be sensitive only in some countries.

The extent, locus, and character of Internet filtering varies from state to state and over time. Web filtering is inconsistent. Web content is constantly changing, which poses a problem for the censors. Mobile devices and social networks have further complicated the task of speech regulation online. No state we have yet studied, even China, seems able to carry out its Web filtering in a comprehensive manner, *i.e.* consistently blocking access to a range of sites meeting specified criteria. China appears to be the most nimble of the states that we have studied at responding to the shifting Web, likely reflecting a devotion of the most resources and political will to the enterprise of technical Internet filtering.

It would be a mistake to infer that Internet filtering is only a phenomenon that takes place in states with histories of hostility to free expression. Democratic states participate in extensive regulation of the Internet, just as authoritarian states do. We have documented extensive Internet filtering in northern Europe, for instance, associated with child pornography. In the United States, the state regulates what children can see in libraries and schools, as one means of limiting access to information deemed to be harmful to them. One may feel differently about these child protection measures than one does about the blocking of speech by activists on the fringe of non-democratic societies, but the practices involve similar technical mechanisms in both types of settings.

A state wishing to filter its citizens' access to the Internet has several initial options: DNS filtering, IP filtering, or URL filtering. Most states with advanced filtering regimes implement URL filtering, as it can avoid even more drastic overfiltering or underfiltering

situations. In the case of overfiltering, states block more than is necessary to achieve the regulatory purposes, such as blocking all blogs on WordPress (in the case of Turkey) or all usage of the social network Facebook (in Pakistan), when the offending material could be targeted and blocked precisely and without limiting the expression of non-offenders. To implement URL filtering, a state must first identify where to place the filters; if the state directly controls the ISP(s), the answer is straightforward. Otherwise, the state may require private or semi-private ISPs to implement the blocking as part of their service. The technical complexities presented by URL filtering become non-trivial as the number of users grows to millions rather than tens of thousands. Some states appear to have limited overall access to the Internet in order to keep URL filtering manageable. The government of Saudi Arabia, for example, made the ability to filter a pre-requisite of public Internet access, delaying any such access for a period of several years until the resources to filter were set in place.

Citizens with technical knowledge can generally circumvent filters that a state has put in place. Some states acknowledge as much: the overseer of Saudi Arabia's filtering program, via the state-run Internet Services Unit, admits that technically savvy users can simply not be stopped from accessing blocked content. Expatriates in China, as well as those citizens who resist the state's control, frequently find up-to-date proxy servers through which to connect to the Internet and through which they can evade filters in the process. While no state will ultimately win a game of cat-and-mouse with those citizens who are resourceful and dedicated enough to employ circumvention measures, a

preponderance of users will never do so—rendering filtering regimes at least partially effective despite the obvious workarounds.

Some of the earliest theorizing about control in the online environment, from the “open net” period, suggested that such state-run control of Internet activity would not work. States such as China have proven that an ambitious regulatory body can, by devoting substantial technical, financial, and human resources, exert a large measure of control over what their citizens do online. States, if they want, can erect digital gates at their borders, even in cyberspace, and can render these gates effective through a wide variety of modes of control. (Lessig 2000; Goldsmith and Wu 2006: 65 - 86) These controls have proven right the claims of Lawrence Lessig, Jack L. Goldsmith and others who have emphasized the extent to which the online environment can be regulated and the ways in which traditional international relations theory will govern in cyberspace as in real-space. (Goldsmith 2003)

Phase 3: Access Controlled (2005 to 2010).

The third phase, from 2005 roughly to the present day, is the “access controlled” phase. Access controlled characterizes a period during which states have emphasized regulatory approaches that function not only like filters or blocks, but also as variable controls. The salient feature of this phase is the notion that there are a large series of mechanisms, at a variety of points of control, that can be used to limit access to knowledge and information. These mechanisms can be layered on top of the basic filters and blocks

established during the previous era. (Deibert and Rohozinski, in Deibert et al. 2010: 3 - 12.)

The mechanisms of the Access Controlled period are more subtle and nuanced than the first-generation filtering and blocking mechanisms that they complement. These controls can change over time to respond to changing political and cultural environments that arise online and offline. Filtering mechanisms can be made to work just-in-time, in order to block content and services at politically sensitive moments, as the Chinese have done in the lead-up to the anniversary of the Tiananmen Square protests in 2009. Many states also use registration, licensing, and identity requirements to control what people do online. In order to publish information lawfully on the Internet, one needs to register oneself with the state as a publisher. The first-order controls associated with censorship are combined with legal controls and surveillance, the effect of which is to ensure that those publishing online know that they are being watched and that the state is capable of shutting them down – or putting them in jail. These methods of regulation, working in combination, are highly effective, both as a means of law enforcement and through a chilling effect on online speech. (Deibert and Rohozinski, in Deibert et al. 2010. 24 – 28)

During this Access Controlled period, states have also increased the number of points of control that are possible on this network and their use in combination. The image of the “Great Firewall of China” is evocative and, to some extent, accurate as a descriptive matter. But it is misleading insofar as it tells only a small part of the story of control

online, in China and elsewhere. States control the online environment not just at the national border, as information flows in and out of the state, but in many environments within states. For instance, in order to go into a cyber café to log on to the Internet in Turkey, one has to prove one's identity, log in at the front of the store so that the proprietor can link your online activities to a certain machine and IP address and period of time. These registration and logging requirements are combined with surveillance cameras that are trained on the computer users in the cyber cafés. Law enforcement officials, in turn, can monitor or later recreate the digital tracks of the large population of Internet users who rely upon cyber cafés, especially in developing countries where fast Internet to the home is prohibitively expensive or non-existent.

States themselves cannot implement the level of control that they seek over activity the network directly, so their control strategies have expanded to include pressure on private parties. Soon after China erected its Great Firewall, it became clear that this approach would not be sufficient as a means of exercising the extent and kinds of control that the state wanted to carry out over time. It has turned to private companies like Google to do most of the blocking or the surveillance for them, leading to a highly public, multi-year showdown between the state's regulators and the company's executives. China has also turned to Yahoo! to demand that its staff hand over information about a Hong Kong-based journalist who is using the Yahoo! email service.

We are living in a hybrid world, where the online and the offline are deeply connected.

States exercise control at an increasing number of these points of interconnection, whether through mobile devices, access points at library and schools, and in workplaces. Internet service providers play a central role in many control strategies for states. As we wrap more and more of our lives into this meshed environment, the points of control for states continue to grow as well.

Phase 4: Access Contested (2010 and beyond).

Today, circa 2010, we are headed into a fourth phase, called “access contested.” The key notion behind this new phase is that there is, and will be more, pushback against some of these controls. There is an ongoing contest over what this hybrid environment will look like over time. There is a growing political debate about the way in which these regulations are carried out by states around the world. At a state-to-state level, the militarization of cyberspace that has been happening over the last few years is an important part of this emerging narrative.

The growing centrality of activities online to life in general is the primary driver of these contests. From the perspective of Internet users, online activity is increasingly a part of everyday life – not a separate sphere to which they travel occasionally, as if on vacation. States, too, have come to recognize that activities mediated by digital technologies are deeply important in economic, political, and cultural ways as a critical mass of their citizens, businesses, and NGOs come online. The metaphor of “cyberspace” as a space, akin to “real space,” breaks down in this respect. The technological mediation of these

activities changes some things – for instance, the technology brings with it specific affordances for the activist in getting her word out and the spy in snooping on Internet traffic as it passes – but it does not change the underlying dynamics of states, companies, individuals, and groups.

In the “access contested” phase, the regulation that states have imposed in the earlier phases is giving rise to strong responses from the private sector and from other states unhappy with this regulation. Companies are implementing new strategies for coping with the spread of regulation and liability that they face as Internet intermediaries. In response to mounting pressure from states including China and Vietnam, companies such as Google, Microsoft, and Yahoo! have joined together with human rights groups and academics to establish an organization, the Global Network Initiative, to help implement a code of conduct for handling such demands in a manner than upholds civil liberties. (Global Network Initiative 2010) And companies compete, directly and indirectly, in how extensively they carry out censorship online. Search engines, for instance, vary in terms of how and to what extent they filter keywords. Microsoft’s Bing filters keyword searches related to sexuality and gay and lesbian matters in the Middle East and elsewhere in the world in manners different from their competitors and different from their United States-based service. (Noman 2010) Regulation online is increasingly a blend of the public and the private. (Palfrey and Zittrain, in Deibert et al. 2008: 103-122; Maclay, in Deibert et al. 2010: 87-108)

States, too, are now actively engaged in a contest with one another over cyberspace. Military officials increasingly think of the online environment as a strategic domain and a potential zone of warfare. The militarization of cyberspace describes the manner in which states have built up offensive information warfare capabilities in recent years. (Deibert in Boler, ed. 2008: 152 – 157) The Information Warfare Monitor, a project of the Citizen Lab at the University of Toronto, tracks these developments and conflicts as they arise. (Information Warfare Monitor 2010)

Public reaction to Internet regulation also points to the contest that is beginning to play out in public arenas around the world. Demonstrators in Pakistan in 2010 made plain their disagreement with the state's decision to increase the incidence of Internet blocking. China's mandate that hardware providers install Green Dam filtering software on new computers before they shipped met with substantial resistance and was pulled back. The Malaysian state has publicly struggled with political pressure to start filtering. Plans to institute state-mandated filtering in Australia were shelved after extensive public pushback. The last chapter has yet to be written in the back-and-forth between Google and China about whether unfiltered search results may be presented to Chinese Internet users. And in contrast to most other examples, there appears to be vocal public support in favor of pornography filtering in Indonesia. (OpenNet Initiative Blog 2010) These and many other contests like them will play out in the years to come.

Looking Ahead: Competing Modes of Regulation.

The perspective of most states on Internet regulation has changed substantially from where it began in the “open net” era. The premise today is not whether the Internet can be regulated, but rather how it must be regulated and how that regulation should be carried out most effectively. States also have come to realize that the activities of other states online need to be constrained in various respects. State interests in what transpires online – the activities of other states, private companies, individuals and groups – have become much clearer over the past decade.

The early theorizing about Internet regulation centered on the extent to which states could, and would, regulate the activities of individuals in cyberspace. (Johnson and Post 1996) This kind of state-to-individual regulation is a given today. Contests now center on other kinds of regulation. First, states are regulating private companies, both to constrain what those companies can do directly and to require that these companies carry out control of individuals. Second, states are considering how to limit what companies based in their jurisdiction (for instance, all the technology companies chartered in the United States) can do in other countries, as a means of pushing back against the regulatory actions of other states. And third, states are striving to find ways to limit what other states may do by way of activity on the Internet. These multiple layers of regulation may prove to make activities on the Internet more, not less, subject to complex controls by states than offline activities. A key feature of the Access Controlled period will be the interplay between these often competing forms of regulation.

Over the past few decades, the world wide web has gone from an “open net,” characterized primarily by the freedoms it afforded, to a hotly contested environment, characterized by the political battles that rage upon it. What was once known as “cyberspace” is now an environment in which debates fly, activism flourishes and fails, and political and military contests play out between states. The Internet has always been a network that could be regulated. It has also always been a network that could support an expansion of the freedom of expression and association, especially for those living in regimes where the public media environment has been historically constrained.

The question about Internet regulation, looking forward, needs to be inverted. Instead of asking whether the Internet can be regulated, the question should be whether it will be regulated in precisely the same way, or more extensively, than the offline world as the stakes rise in the Access Contested era.

References:

Barlow, John Perry. "A Declaration of the Independence of Cyberspace." February 8, 1996. <https://projects.eff.org/~barlow/Declaration-Final.html>

Benkler, Yochai. *The Wealth of Networks*. New Haven: Yale University Press, 2005.

Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds. *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge, MA: MIT Press, 2008.

Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT Press, 2010.

Deibert, Ronald. "Black Code Redux: Censorship, Surveillance, and the Militarization of Cyberspace." *Digital media and democracy: tactics in hard times*. Ed. Megan Boler. Cambridge, MA: MIT Press, 2008.

Etling, Bruce, John Kelly, Rob Faris, and John Palfrey. "Mapping the Arabic Blogosphere: Politics, Culture and Dissent." Berkman Center Publications Series. June 16, 2009. http://cyber.law.harvard.edu/publications/2009/Mapping_the_Arabic_Blogosphere

Global Network Initiative. <http://www.globalnetworkinitiative.org>

Global Voices Online. <http://www.globalvoicesonline.org>

Jack L. Goldsmith. “Against Cyberanarchy.” *Who Rules the Net?: Internet Governance and Jurisdiction*. Ed. Adam Thierer et al. Washington, DC: Cato Institute, 2003.

Jack L. Goldsmith and Tim Wu, *Who Controls the Internet: Illusions of a Borderless World*. Oxford: Oxford University Press, 2006.

Information Warfare Monitor. <http://www.infowar-monitor.net/>

Johnson, David R. and David G. Post. “Law and Borders - The Rise of Law in Cyberspace.” *Stanford Law Review*, Vol. 48, p. 1367, 1996. Available at SSRN: <http://ssrn.com/abstract=535> or doi:10.2139/ssrn.535

Kelly, John and Bruce Etling. “Mapping Iran’s Online Public: Politics and Culture in the Persian Blogosphere.” Berkman Center Publications Series. April 5, 2008. http://cyber.law.harvard.edu/publications/2008/Mapping_Irans_Online_Public

Lawrence Lessig. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.

Noman, Helmi. "Sex, Social Mores, and Keyword Filtering: Microsoft Bing in the 'Arabian Countries'". OpenNet Initiative Bulletin. January, 2010.
<http://opennet.net/sex-social-mores-and-keyword-filtering-microsoft-bing-arabian-countries>

Noveck, Beth. *Wiki Government: How Technology Can Make Government Better, Democracy Stronger, and Citizens More Powerful*. Washington, DC: Brookings Institution Press, 2009.

The OpenNet Initiative. <http://www.opennet.net>.

The OpenNet Initiative Blog. <http://opennet.net/blog/2010/08/indonesia-and-its-porn-troubles>

Rheingold, Howard. *Smart Mobs: The Next Social Revolution*. New York: Basic Books, 2003.