1 Beyond Denial

Introducing Next-Generation Information Access Controls

Ronald Deibert and Rafal Rohozinski

Introduction

It is hard to imagine the world before the Internet. A generation of digital natives has grown up with ubiquitous connectivity, where neither borders nor language seems a barrier to communication.[1] And yet, less than 20 years ago the global information environment was a much more controlled and regulated space, organized around sovereign states. Throughout much of modern history, governments have wrestled with the tensions of the relentless drive to build new technologies and the unpredictable and often counterproductive consequences that flow from them for their power and authority.[2] No less of a historical figure than Stalin captured this tension between the quest for modernity and the compulsion to control. When presented with a proposal to build a modern telephone system for the new Soviet state, he reportedly replied, "I can imagine no greater instrument of counterrevolution in our time."

The rise of the Internet coincided with a major set of political upheavals that culminated with the collapse of the Soviet Union and communist bloc. In the euphoria that ensued, the idea of technological redemption, inevitable democratization, and for some, the end of history, coalesced into a popular ideology that equated technology with empowerment. This idea was far from new. Indeed, the telegraph, electrical lighting, and telephony all emerged at similarly transformational historical junctures, leading to a long pedigree of speculation regarding the democratizing role of technology in social and political change.[3]

There is no doubt that the Internet has unleashed a wide-ranging and globally significant shift in communications—a shift that has led to the empowerment of individuals and nonstate actors on an unprecedented scale. At times, the Internet seems uncontrollable, a constantly evolving and dynamic virtual realm, reshaped continuously by a growing number of users at edge points of the network. But Newtonian physics is as relevant in politics and cyberspace as it is in the physical realm. Just as with previous technological developments, as the Internet has grown in political significance, an architecture of control—through technology, regulation, norms, and political calculus —has emerged to shape a new geopolitical information landscape.

In 2008, the OpenNet Initiative (ONI) published its first global study—*Access Denied: The Practice and Policy of Global Internet Filtering*[4]—which documented how states are seeking to establish borders in cyberspace. Our snapshot of 41 countries discovered that states were busy constructing defensive perimeters to deny access to unwanted content. For the most part, these methods consisted of building firewalls at key Internet choke points. The People's Republic of China was among the first to adopt national filtering systems at the backbone of the country's Internet—popularly known as the ''Great Firewall of China''—and it has become a paradigm of Internet censorship ever since. ''Chinese-style'' filtering—as we call it here—represents the *first generation* of Internet control techniques.

In Chinese-style filtering, lists of Internet protocol (IP) addresses, keywords, and/or domains are programmed into routers or software packages that are situated at key Internet choke points, typically at international gateways or among major Internet service providers (ISPs).[5] Requests that are made for any information contained in the block lists are denied for citizens living within those jurisdictions. The latter can happen in a variety of ways, with greater and lesser degrees of transparency, but it is almost always static, fixed in time, and relatively easy to discern using the methods developed over time by the OpenNet Initiative's researchers (see box on ONI's methodology). Moreover, determined Internet users can circumvent them with relative ease.

Not all countries have been as forthright with their rationale for filtering Internet content as China. Our research for *Access Denied* also found coyness on the part of many states to admit seeking to control Internet content. In many cases, denial of access occurred extralegally, or under the guise of opaque national security laws. Often, ISPs were simply asked or told to block access to specific content without any reference to existing law. Other times, blockages were difficult to distinguish from network errors or other technical problems, like denial of service attacks, but seemed suspiciously connected to political events. Many of the countries listed in our first report denied that they were in fact blocking access to Internet content or had any connection to attacks on services. We saw these events as anomalies insofar as they did not fit the paradigm of Chinese style filtering and largely eluded the methodologies that we had developed to test for Internet censorship.[6]

We have subsequently come to learn that these anomalies were, in fact, emerging norms. Since our research for *Access Denied* was conducted, a sea change has occurred in the policies and practices of Internet controls. States no longer fear pariah status by openly declaring their intent to regulate and control cyberspace. The convenient rubric of terrorism, child pornography, and cyber security has contributed to a growing expectation that states should enforce order in cyberspace, including policing unwanted content. Paradoxically, advanced democratic states within the Organization for Secu-

Box 1.1

The ONI employs a unique ''fusion'' methodology that combines field investigations, technical reconnaissance, and data mining, fusion, analysis, and visualization. Our aim is to uncover evidence of Internet content filtering in countries under investigation. The ONI's tests consist of running special software programs within countries under investigation that connect back to databases that contain lists of thousands of URLs, IPs, and keywords. The lists are broken down into two categories: global lists include URLs, IPs, and keywords that are tested in every country, and which help us make general comparisons of accessibility across countries. Global lists also provide a ''snapshot'' of accessibility to content typically blocked by filtering software programs, and can help us understand whether particular software programs are being used in a specific context. Local lists are unique for each country and are usually made up of content in local languages. These are high-impact URLs, IPs, and keywords, meaning they are content that is likely to, or has been reported to have been, targeted for filtering. Our aim is to run tests on each of the main ISPs in a country over an extended period of time—typically at least two weeks on at least two occasions. Our accessibility depends very much on our in-country testers, and for security and other reasons we are not always able to perform comprehensive tests, meaning in some cases we have only partial results on which to make inferences. Our specially designed software checks access both within the country and from one or more control locations simultaneously. Anomalies are analyzed and determinations are made as to whether a site is accessible or not, and if the latter, how the inaccessibility occurs. In some instances, block-pages—Web sites that explicitly confirm blocking—are yielded for requests for banned content. In other instances, connections are simply broken. In some cases, special filtering software is employed, while in others routers are manually configured to block.

rity and Cooperation in Europe (OSCE)—including members of the European Union (EU)—are (perhaps unintentionally) leading the way toward the establishment of a global norm around filtering of political content with the introduction of proposals to censor hate speech and militant Islamic content on the Internet. This follows already existing measures in the UK, Canada, and elsewhere aimed at eliminating access to child pornography. Recently and amid great controversy, Australia announced plans to create a nationwide filtering system for Internet connectivity in that country. Although the proposal has ultimately languished, it shows the extent of this growing norm. No longer is consideration of state-sanctioned Internet censorship confined to authoritarian regimes or hidden from public view. Internet censorship is becoming a global norm.

At the same time, states have also become more cognizant of the strategic importance of cyberspace (of which the Internet is an important constituent component). Cyberspace has become militarized. A clever use of the Internet by insurgents and militants in Iraq and other parts of the Middle East, the significance of the Internet in conflicts such as the 2008 Russia-Georgia war, and revelations concerning large-scale cyber-espionage networks,[7] has emphasized the impact of cyberspace on the *sweat and muscle* aspects of war fighting, and geopolitical competition among states and nonstate actors. Reflecting on these recent incidents, many states' armed forces and policymakers have engaged in a fundamental rethinking of assumptions about the importance of the informational domain to conflict and competition. As a consequence, states are now openly pursuing a cyber arms race with leading powers such as the United States, Russia, and China unashamedly making their intentions clear in doctrines for military engagement in cyberspace. The quest for information control is now *beyond denial*.

The present volume aims to document, analyze, and explore these emerging next-generation techniques, what they mean for relationships between citizens and states, and how they will shape cyberspace as a domain for civic interaction into the future. The title of our volume—*Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*—suggests how the *center of gravity* of practices aimed at managing cyberspace has shifted subtly from policies and practices aimed at denying access to content to methods that seek to *normalize* control and the exercise of power in cyberspace through a variety of means.

This volume differs from its predecessors in two ways. First, our focus is primarily on the 56 countries that make up the OSCE. This is a deliberate choice, as many of the legal mechanisms that legitimate control over cyberspace, and its militarization, are led by the advanced democratic countries of Europe and North America. Likewise, many of the more innovative means by which laws and techniques used to silence voices in cyberspace are emerging from the postcommunist countries of the Commonwealth of Independent States (CIS). In this respect, the industrialized North is establishing norms that are only too readily propagated and adopted by repressive and authoritarian regimes elsewhere.

Second, *Access Controlled* focuses on the new generations of Internet controls that go beyond mere denial of information. Whereas Chinese-style national filtering schemes represent the first generation of Internet filtering, second- and third-generation techniques are more subtle, flexible, and even offensive in character. These next-generation techniques employ the use of legal regulations to supplement or legitimize technical filtering measures, extralegal or covert practices, including offensive methods, and the outsourcing or privatizing of controls to "third parties," to restrict what type of information can be posted, hosted, accessed, or communicated online. Examples of next-generation techniques include the infiltration and exploitation of computer systems by targeted viruses and the employment of distributed denial-of-service (DDoS) attacks, surveillance at key choke points of the Internet's infrastructure, legal takedown notices, stifling terms-of-usage policies, and national information-shaping strategies, all of which are highlighted in one way or another in the chapters that follow. Although these measures may have the same aim as Chinese-style filtering, they reflect a maturation of methods resulting from a growing colonization of cyberspace by states and other actors. They emerge from a desire to *shape* and *influence* as much as tightly *control* national and global populations that are increasingly reliant on cyberspace as their main source of information. These next-generation controls raise important and sometimes troubling public policy issues—particularly for the relationship between citizens and states.

Chapter Overview

Second- and third-generation controls are carefully defined in our subsequent chapter in this volume, *Control and Subversion in Russian Cyberspace*. Second-generation controls create a legal and normative environment and technical capabilities that enable actors to deny access to information resources as and when needed, while reducing the possibility of blowback or discovery. These controls have an overt and covert track. The overt track aims to legalize content controls by specifying the conditions under which they can be denied. Instruments here include the doctrine of information security as well as the application of existent laws, such as slander and defamation, to the online environment. The covert track establishes procedures and technical capabilities that allow content controls to be applied "just in time," when the information being targeted has the highest value (e.g., during elections or public demonstrations), and to be applied in ways that assure plausible deniability.

Third-generation controls take a highly sophisticated, multidimensional approach to enhancing state control over national cyberspace and building capabilities for competing in informational space with potential adversaries and competitors. The key characteristic of third-generation controls is that the focus is less on denying access than successfully competing with potential threats through effective counterinformation campaigns that overwhelm, discredit, or demoralize opponents. Third-generation controls also focus on the active use of surveillance and data mining as means to confuse and entrap opponents.

We argue that while the countries of the CIS are often seen as lagging behind Europe, North America, and the technological tigers of Asia, they may be leaders in the development of next-generation controls. Some of the first, and most elaborate, forms of just-in-time blocking, terms-of-usage policies, surveillance, and legal takedown notices occurred among the countries of the CIS over the last several years. Examining that region in detail may give us insight into the future of information controls elsewhere.

Computer network attacks and exploitation—what we called "just-in-time" blocking in *Access Denied*—are perhaps the starkest of examples of next-generation techniques. Computer network attacks describe the range of controls that target and "take down" strategically important sources of information or services at key moments in time through computer-based information attacks. Although there are several tactics that can be employed within this rubric—deliberate tampering with domain name servers, virus and Trojan horse insertion, and even brute physical attacks—the most common is the use of DDoS attacks. These attacks flood a server with illegitimate requests for information from multiple sources—usually from so-called ''zombie'' computers that are infected and employed as part of a ''botnet.'' The ONI has monitored an increasing number of just-in-time blocking incidences using DDoS attacks, going back to our first acquaintance during the Kyrgyzstan parliamentary elections of 2005. In that episode, the Web sites of opposition newspapers came under a debilitating attack that left them unable to communicate during the critical period leading up to and during the Kyrgyz election.[8] Since the Kyrgyz case, DDoS attacks have featured prominently in the dispute between Russia and Estonia in May 2007, during the Russia-Georgia conflict of 2008, and in numerous cases involving the Web sites of human rights and political opposition groups.

These tactics are particularly difficult to monitor using traditional ONI methods because of their temporary and fleeting duration, and because their perpetrators can disguise their involvement through distribution and anonymity. Today, organized criminal networks operate commercial botnets with significant powers of disruption. Perpetrators can simply contract out a DDoS attack and benefit by the convenience of an electronic assault that from the outside may look as though it is a random attack or a series of unfortunate network errors. Attributing such attacks to their source is difficult because the vectors are distributed and the transactions are done through criminal activity and illicit shadow markets. Although much of what the ONI has observed in terms of computer network attacks and just-in-time blocking has occurred in the developing world, it is noteworthy the military use of botnets is being debated in NATO countries and elsewhere.[9] The prospect of an arms race in cyberspace looms large.

Among many countries in the industrialized world, a major impetus to filter is the desire to control access to information relating to the sexual exploitation of children, otherwise known as child pornography. In almost all countries, possession and distribution of child pornography is illegal. In some countries, laws have been enacted to restrict distribution of child pornography online. In some countries, private ISPs have entered into voluntary arrangements to filter access to lists of child pornographic material, while in others entire nationwide filtering schemes have been proposed. In all cases, the proposals have been the subject of considerable public debate and controversy. Although only a few very extreme minority groups, such as libertarians, question the right to access child pornography, many have raised questions about the transparency of the processes being followed or the mechanisms put in place for oversight and review. For the ONI, for example, the mere test for access to this material is prohibited because a simple connection to such a site would constitute a crime in most jurisdictions. This situation leaves many researchers in a quandary as to how to verify that lists are accurate and do not contain collateral filtering problems or categorization mistakes common to filtering software. Nart Villeneuve's chapter provides a historical overview of online child pornography controls and examines the range of policy responses that have been employed. As Villeneuve explains, many governments have adopted national filtering policies rather than developing international information-sharing arrangements that would involve police cooperation and the removal of information at its source.

Another example of next-generation information controls prominent among the countries of the OSCE is the extensive use and application of surveillance. As Hal Roberts and John Palfrey outline in their chapter, surveillance can happen at numerous points throughout the infrastructure of cyberspace and can be collected by a variety of public and private actors who have access to those choke points. States' intelligence and law enforcement agencies are increasingly extracting precious information flows through the installation of permanent eavesdropping equipment at key Internet choke points, such as Internet exchanges, ISPs, or major international peering facilities, and combining such information with new tools of reconnaissance drawn from data sources such as CCTVs, satellite imagery, and powerful systems of geo-locational mapping. To be sure, electronic surveillance is nothing new, having a long history shrouded with secrecy. Throughout the cold war, both superpowers assembled globe-spanning electronic surveillance systems that operated in the most highly classified realms. However, today's surveillance systems are much more extensive and penetrating, and are legitimized by permissive antiterror legislation that removes many previous operational constraints. They are also increasingly operated and controlled not by the state but by private actors. As with just-in-time blocking, surveillance eludes the ONI's methods and is generally quite difficult to monitor using technical means. It is, however, a very powerful force of information control and can create a stifling climate of self-censorship.

Another control beyond denial that is profiled in *Access Controlled* relates to the growing and widespread prevalence of cyberspace as a communications environment, and the ways in which third-party intermediaries, including private companies and public institutions, host, service, and ultimately control that environment. At one point in time, it might have been fair to characterize cyberspace as largely a separate and distinct realm—something people "enter into" when they turn on their computers or play video games. Today, however, with always-on portable devices that are fully connected to the Internet, and much of society's transactions mediated through information and communication technologies—including business, work, government, and play—cyberspace is not so much a distinct realm as it is the very environment we inhabit. Our lives have been digitally disassembled, disaggregated, and dispersed into multiple digital domains. Our "private" information now traverses through cables and spectrum owned and operated by numerous private and public institutions located in numerous legal jurisdictions. The same is true of government and business information. It is hosted on servers each of which may have unique terms-of-service, data-retention, and use policies. Depending on the territorial jurisdiction in which they are located, they may be subject to the pressures of law enforcement and intelligence to turn over that information, either overtly or covertly. And they are subject to a bewildering variety of local, national, and international laws, some of which may conflict.

Issues of censorship that involve terms-of-use policies, takedown notices, and other commercial compliance and service issues are taken up in both the Ethan Zuckerman and Colin Maclay chapters. Zuckerman outlines some of the ways in which competitive market forces can create unintended consequences leading to censorship by ISPs and online service providers (OSPs). Unwilling or afraid to bear the burden of legal and other costs of hosting controversial information, ISPs and OSPs may simply err on the side of caution, leading to a situation where the spaces for hosting content deemed objectionable anywhere are progressively winnowed. As much of what happens online today, from e-mail to documentation to chats, flows through or otherwise depends on these large ''cloud'' services managed by private companies, such a chilling effect could have profound consequences on freedom of speech and access to information.

Maclay's chapter focuses on issues of accountability and transparency around OSPs and ISPs that operate or provide services in jurisdictions where Internet censorship takes place. In many countries, Internet companies are either pressured or legally compelled to censor their services or turn over user data, with search engines being among the most common of them. In China, for example, major search engine companies all filter their search results, and at least one has turned over personal data to Chinese authorities, resulting in arrests. These practices have garnered significant controversy, particularly in the United States where the largest of them—Microsoft, Yahoo!, Google—are based. In an effort to forestall legislation that would restrict their investment practices abroad, these companies have entered into a self-regulation pact, called the Global Network Initiative, which Maclay analyzes and discusses. Given that much of cyberspace is operated by the private sector, such self-regulation pacts may become a more common feature of cyberspace governance, as will undoubtedly the policing of Internet content controls.

Conclusion

The trends and findings analyzed in *Access Controlled* reveal a rapidly emerging normative terrain that should be of concern to policymakers, advocacy and rights networks, and academics. Given the strategic importance of the OSCE, in terms of relative military capabilities, wealth, and diplomatic influence, the norms emerging from this region are bound to have unintended consequences all over the world. Understanding those impacts will be of paramount importance for Internet governance at all levels in years to come.

Probably the most important norm is the ''security first'' orientation toward Internet governance, driven in part by the fear of terrorism and in part by concerns of protecting vulnerable populations (particularly children) from exploitation. Across the OSCE, communities of practice in law enforcement, intelligence, and the private sector are working, often in uncoordinated, discrete, but like-minded ways, leading to a normalization of Internet surveillance and censorship across all sectors of cyberspace. It is perhaps ironic that these norms so antithetical to basic rights and freedoms are being propagated from many countries that just over a decade ago were responsible for the expansion of liberal democratic principles and market capitalism across the globe. And yet upon closer consideration such trends conform to what have been called ''governmentality practices'' in general that characterize these societies, as techniques of control become progressively more refined, technologically rigorous, and bureaucratically complex. Although not ''socially sinister,'' as David Lyons puts it, what he calls ''everyday surveillance'' has routinized itself into ordinary life in so many myriad ways that it has become the taken-for-granted context within which modern industrialized society operates.[10] The security-first norm around Internet governance can be seen, therefore, as but another manifestation of these wider developments. Internet censorship and surveillance—once largely confined to authoritarian regimes—is now fast becoming the global norm.

But there is a second characteristic of this newly emerging normative terrain that is unique to cyberspace and the speed with which such changes are being wrought, in particular to the long-standing pillars of modern citizen-state relations. The ''social contract'' that has set the basic framework for citizen-state relations in the modern industrialized period has been shaped by decades of technological and social change and institutional innovations. One must be careful, therefore, to ascribe to contemporary events unique and epochal challenges. However, the way in which citizen-state relations are being upset in a very compressed time frame is worth noting, and may be comparable only to that which happened at the height of the industrial revolution itself. In such a context of rapid technological and social change, the margin for error and unintended consequence around laws and regulations is enormous as path dependencies open up around fast-moving developments that only in hindsight can be identified as such.

The salience of such impacts can be seen in the practices surrounding the distributed ownership infrastructure of cyberspace. Today, peoples' everyday lives are mediated not only through the state per se, but dispersed through clouds of digital-electronic telecommunications owned and operated by private entities. Each of these clouds—often spanning multiple national jurisdictions—represents potential, and often actual, loci of private authority. As shown throughout each of the chapters in this volume, the decisions they make on when to retain, filter, monitor, and share the information they control (and with whom) are increasingly having important political ramifications for citizens the world over. The normative terrain outlined in *Access Controlled* thus offers a compelling example of the privatization of authority.

Perhaps the most important unintended consequences may come from new conflicts and offensive operations documented in this volume. The growing acceptance of the militarization of cyberspace, by states and by third-party actors, risks significant blowbacks as these techniques—once hidden from view or confined to marginalized contexts—become an entrenched characteristic of global relations. Societies around the world—none more so than those of the OSCE—are heavily dependent on globally networked technologies. They have been locked in and interpenetrated by a digital web of their own spinning.[11] And so from a rational perspective, an arms race in cyberspace is to no one's advantage; a collapse of one information infrastructure would undoubtedly affect others—perhaps even the perpetrator. But as so often is the case in the competitive dynamics of world politics, the logic of security dilemmas can easily overwhelm and entrap rational decision-making processes. Today, governments are responding to the threats of cyberwar not by pursuing norms of mutual restraint but by endorsing new techniques of offensive operations, including outsourcing to third-party actors and criminal organizations.

Last, this newly emerging normative terrain of next-generation Internet controls presents major challenges to monitoring organizations, including the ONI itself. The technical investigations that informed our country studies and that are reported on here represent a methodology borne out of the need to monitor first-generation technical filtering techniques. If the trends identified in *Access Controlled* are accurate, then these first-generation filtering techniques may be gradually superseded by a variety of next-generation controls that are more subtle and fluid and deeply integrated into social relations rather than fixed at specific choke points. This possibility suggests that the ONI itself must now respond with a new suite of methodologies if it hopes to remain relevant to the challenges of cyberspace governance that lay ahead.

Notes

1. John Palfrey and Urs Gasser, *Born Digital: Understanding the First Generation of Digital Natives* (New York: Basic Books, 2008).

2. Unpredictable consequences of technological change is a theme explored in Ronald J. Deibert, *Parchment, Printing and Hypermedia: Modes of Communication in World Order Transformation* (New York: Columbia University Press, 1997).

3. Tom Standage, *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-line Producers* (New York: Berkeley Books, 1998).

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

5. Steven J. Murdoch and Ross Anderson, "Tools and Technology of Internet Filtering," in *Access Denied: The Practice and Policy of Global Internet Filtering*, ed. Ronald J. Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2008), 57–72.

6. Ronald J. Deibert and Rafal Rohozinski, "Good for Liberty, Bad for Security? Global Civil Society and the Securitizaton of the Internet," in *Access Denied: The Practice and Policy of Global Internet Filtering*, ed. Ronald J. Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2008), 123–149.

7. Information Warfare Monitor, "Tracking GhostNet: Investigating a Cyber Espionage Network," Citizen Lab/the SecDev Group, March 29, 2009, http://www.tracking-ghost.net.

8. OpenNet Initiative, "Special Report: Kyrgyzstan, Election Monitoring in Kyrgyzstan," April 15, 2005, http://www.opennetinitiative.net/special/kg/.

9. For example, see Col. Charles W. Williamson III, "Carpet Bombing in Cyberspace: Why America Needs a Military Botnet," *Armed Forces Journal* (May 2008), http://www.armedforcesjournal.com/2008/05/3375884.

10. David Lyons, *Surveillance Society: Monitoring Everyday Life* (Buckingham, UK: Open University Press, 2001).

11. Ronald J. Deibert, "Network Power," in *The Political Economy of a Changing Global Order*, 2nd ed., ed. Richard Stubbs and Geoffrey Underhill (New York: Oxford University Press, 1999).