2

Internet Filtering: The Politics and Mechanisms of Control

Jonathan Zittrain and John Palfrey

It seems hard to believe that a free, online encyclopedia that anyone can edit at any time could matter much to anyone. But just as a bee can fly despite its awkward physiognomy, Wikipedia has become wildly popular and enormously influential despite its unusual format. The topics that Wikipedians write about range more broadly than any other encyclopedia known to humankind. It has more than 4.6 million articles comprising more than a billion words in two hundred languages.[1] Many Google search queries will lead to a Wikipedia page among the top search results. Articles in Wikipedia cover the Tiananmen Square protests of 1989, the Dalai Lama, the International Tibet Independence Movement, and the Taiwan independence movement. Appearing both in the English and the Chinese language versions of Wikipedia—each independently written—these articles have been written to speak from what Wikipedia calls a ''neutral point of view.''[2] The Wikipedians' point of view on some topics probably does not seem so neutral to the Chinese authorities.

Wikipedia has grown so influential, in fact, that it has attracted the attention of China's censors at least three times between 2004 and 2006.[3]

The blocking and unblocking of Wikipedia in China—as with all other filtering in China, without announcement or acknowledgment—might also be grounded in a fear of the communal, critical process that Wikipedia represents. The purpose of Wikipedia is ''to create and distribute a multilingual free encyclopedia of the highest quality to every single person on the planet in their own language,''[4] and the means of creating it is through engagement of the public at large to contribute what it knows and to debate in earnest where beliefs differ, offering sources and arguments in quasiacademic style.

While its decentralization creates well-known stability as a network, this decentralization reflected at the ''content layer'' for the purpose of ascertaining truth might give rise to radical instability at the social level in societies that depend on singular, official stories for their legitimacy. Wikipedia makes it possible for anyone to tell one's own story about what happened—and, more threateningly to a regime intent on controlling the information environment, to compare notes with others in a process designed to elicit truth from competing perspectives. The once stable lock of a regime accustomed to telling its citizenry how things happened—where states have controlled their media environments for a long time—is threatened.

Wikipedia is the poster-story of a new iteration of the Internet, known as the *read-write Web*, or *Web 2.0* in Silicon Valley terms, or the *semantic Web* in MIT terms. This phenomenon—in which consumers of information can also easily be creators—threatens to open and to destabilize political environments that were previously controlled tightly by those in power. In a world where Wikipedia is accessible, citizens not only can read different versions of the story than the version that the state would have them read, they can help to create them. And not just in their own language: as automated translation tools come into their own, they can interact in many languages.

This version of the Internet also continues the process of breaking down geographic barriers between states by allowing information to flow easily from one jurisdiction to another. The editors of a Wikipedia article are telling the story not just for the benefit of their neighbors in their own country, but for anyone in any place to see. The destabilization that Wikipedia makes possible is also a threat to the ability of a given state to control how its own ''brand'' is perceived internationally.

So why and how would the Chinese state block—and then unblock—Wikipedia repeatedly? That question lies at the heart of this book. Internet filtering is a complex topic, easy to see from many vantage points but on which it is hard to get a lasting fix. As a practical matter, it is easy for a state to carry out technical Internet filtering at a simple level, but very tricky—if not plain impossible—for a state to accomplish in a thorough manner. As a policy matter, are states putting in place filtering regimes because they are concerned that their own citizens will learn something they should not learn? Or that their citizens will say something they should not say? Or that someone in another state will read something bad about the state that is filtering the Net? Where is filtering merely a ministerial task, taken on because the state bureaucracy feels it must at least look like it is making an effort, and where is it a central instrument of policy, initiated if not orchestrated at the highest levels of power?

As a normative matter, broad, informal Internet filtering seems like an infringement of the civil liberties—or, put more forcefully, the human rights—of all of us who use the free, public, unitary, global network of networks that the Internet constitutes. But states have a strong argument that they have the right to control domestic matters, whether or not they occur in cyberspace, and there is often little that other states can do to influence them. The future of the Internet, if not all geopolitics, hangs in the balance.

We are still in the early stages of the struggle for control on the Internet. Early theorists, reflecting the libertarian streak that runs deep through the hacker community, suggested that the Internet would be hard to regulate. Cyberspace might prove to be an alternate jurisdiction that the long arm of the state could not reach. Online actors, the theory went, need pay little heed to the claims to sovereignty over their actions by traditional states based in real space.

As it turns out, states have not found it so very hard to assert sovereignty when and where they have felt the need to do so. The result is the emergence of an increasingly balkanized

Internet. Instead of a World Wide Web, as the data from our study of Internet filtering makes plain, it is more accurate to say we have a Saudi Wide Web, an Uzbek Wide Web, a Pakistani Wide Web, a Thai Wide Web, and so forth. The theory of ''unregulability'' no longer has currency, if ever it did. Many scholars have described the present reality of the reassertion of state control online, despite continued hopes that the Internet community itself might self-regulate in new and compelling ways.[5]

A key aspect of control online—and one that we prove empirically through our global study of Internet filtering—is that states have, on an individual basis, defied the cyberlibertarians by asserting control over the online acts of their own citizens in their home states. The manner in which this control is exercised varies. Sometimes the law pressures citizens to refrain from performing a certain activity online, such as accessing or publishing certain material. Sometimes the state takes control into its own hands by erecting technological or other barriers within its confines to stop the flow of bits from one recipient to another. Increasingly, though, the state is turning to private parties to carry out the control online. Many times, those private parties are corporations chartered locally or individual citizens who live in that jurisdiction. In chapter 5, we describe a related, emerging problem, in which the state requires private intermediaries whose services connect one online actor to another to participate in online censorship and surveillance as a cost of doing business in that state.

The dynamic of control online has changed greatly over the past ten years, and it is almost certain to change just as dramatically in the ten years to come. The technologies and politics of control of the Internet remain in flux. As one example of this continued uncertainty, participants in the Internet Governance Forum (IGF), an open global body chartered via the process that produced two meetings of the World Summit on the Information Society (WSIS), continue to wrestle with a broad set of unanswered questions related to control of the online environment. At a simple level, the jurisdictional question of who can sue whom (and where that lawsuit should be heard, and under the law of which jurisdiction decided, for that matter), remains largely unresolved, despite a growing body of case law. A series of highly distributed problems—spam, spyware, online fraud—continues to vex law enforcement officials and public policy–makers around the world. Intellectual property law continues to grow in complexity, despite some degree of harmonization underway among competing regimes. Each of these problems leaves many unresolved issues of global public policy in its wake. Internet filtering, the core focus of this book, and the related matter of online surveillance, present an equally, if not more, fraught set of issues for global diplomats to address.

Suppressing and Controlling Information on the Internet

The idea that states would seek to control the information environment within their borders is nothing new. Freedom of expression has never been absolute, even in those liberal democracies that hold these freedoms most dear. The same is true of the related freedoms of

association, religion, and privacy. Most states that have been serious about controlling the information environment have done so by holding on to the only megaphones—whether it takes the form of a printing press, a newspaper, a radio station, or a television station—and banning anyone from saying anything potentially subversive.

The rise of the Internet, initially seen as little more than an information delivery mechanism, put pressure on this strategy of control. Early in the twenty-first century, the Saudi state was one of the first to grapple publicly with what the introduction of the Internet might mean. Rather than introducing the Internet in its unfettered—and fundamentally Western—form, the Saudi authorities decided to establish a system whereby they could stop their citizens from accessing certain materials produced and published from elsewhere in the world. As an extension of its longstanding traditional media controls, the Saudis set up a technical means of filtering the Internet, buttressed by a series of legal and normative controls. All Internet traffic to and from Saudi citizens had to pass through a single gateway to the outside world. At that gateway, the Saudi state established a technical filtering mechanism. If Saudi citizens sought to access a Web page that earlier had been found to include a pornographic image, for instance, the computers at the gateway would send back a message telling them, in Arabic, that they have sought to access a forbidden page—and, of course, not rendering the requested page. At a fundamental level, this basic form of control was initially about blocking access to information that would be culturally and politically sensitive to the state.

The issue that the Saudi state faces, of desiring to keep its citizens from accessing subversive content online, is an issue that more and more states are coming to grips with as the Internet expands. The network now joins more than one billion people around the world. At the same time, new issues are arising that are prompting states to establish Internet filtering mechanisms. The read-write Web, exemplified by Wikipedia and the phenomena of blogging, YouTube, podcasting, and so forth, adds a crucial dimension—and additional complexity—as states now grapple with the ease with which their own citizens are becoming publishers with local, national, and international audiences.

How Internet Filtering Works: Law, Technologies, and Social Norms

When states decide to filter the Internet, the approach generally involves establishing a phalanx of laws and technical measures to block their citizens from accessing or publishing information online. The laws are ordinarily extensions of pre-existing media or telecommunications regulatory regimes. Occasionally, these laws take the form of Internet-specific statutes and regulations. These laws rarely explicitly establish the technical filtering regime, but more commonly establish a framework for restricting certain kinds of content online and banning certain online activities.

There are at least five levels of Internet legal control with respect to content control online.[6] States have employed content restrictions, which disallow citizens from publishing or accessing certain online content. Licensing requirements call for intermediaries to carry out certain

Internet filtering, as well as surveillance activities. Liability placed on Internet service providers and Internet content providers can ensure that intermediaries affirmatively carry out filtering and surveillance without a license requirement. Registration requirements establish the need to gather data about citizens accessing the Internet from a certain IP address, user account, cybercafé location, and so forth. And self-monitoring requirements—coupled with the perception, real or imagined, of online surveillance—prompt individual, corporate, and other users to limit their own access and publication online. At the same time, some states are experiencing international pressure to pass Internet-related laws, including omnibus cybercrime statutes that include reference to eliminating access to certain types of banned sites.[7]

The interplay among these types of regulations is a key aspect of this narrative. China, for instance, bundles Internet content restrictions with its copyright laws. This set of regulations sets a daunting web of requirements in front of anyone who might access the Internet or provide a service to another Internet user. These rules create a pretext that can be used to punish those who exchange undesirable content, even though the law may not be invoked in many instances it might cover—including copyright infringement. Vietnam has taken a similar approach, assigning a number of different relevant ministries and agencies a piece of the responsibility to limit what can be done and accessed online. Much of the legal regulation that empowers state agencies to carry out filtering and surveillance tends to be very broadly and vaguely stated, where it is stated at all.

A theme that runs through this book is that Internet regulation takes many forms—not just technical, not just legal—and that regulation takes place not just in developing economies but in some of the world's most prosperous regimes as well. Vagueness as to what content is banned exists not just in China, Vietnam, and Iran, but also in France and Germany, where the requirement to limit Internet access to certain materials includes a ban on ''propaganda against the democratic constitutional order.''[8] Often, these local legal requirements strike a dissonant chord when set alongside international human rights standards, a topic covered in greater detail, and from two different perspectives, in chapters 5 and 6 of this book.

As our global survey shows, and as Faris and Villeneuve set forth in chapter 1 of this volume, several dozen states have gone beyond a legal ban on citizen publication or access of undesirable material online and have set up technical means of filtering its citizens' access to the Internet. In establishing a technical filtering regime, a state has several initial options: domain name system (DNS) filtering, Internet protocol (IP) address filtering, or URL filtering.[9] Most states with advanced filtering regimes implement URL filtering, as this method can be the most accurate (see ''Filtering and Overbreadth'' section later in this chapter).[10]

To implement URL filtering, a state must first identify where to place the filters. If the state directly controls the Internet service provider(s), the answer is clear. Otherwise, it may require private or semiprivate ISPs to implement the blocking as part of their service. The technical complexities presented by URL filtering become nontrivial as the number of users grows to millions rather than tens of thousands. Some states appear to have limited the number of people

who can access the Internet, as Myanmar has, in order to keep URL filtering manageable—or to be able to shut off access to the network entirely, as the military junta appears to have done in September 2007.

Technical Internet filtering is not perfect in any jurisdiction. Even the most sophisticated technical filtering regimes can have difficulty covering those cases where users are intent on getting or publishing certain information, and willing to invest effort and risk to do so. Every system suffers from at least two shortcomings: a technical filtering system either underblocks or overblocks content, and technically savvy users can circumvent the controls with a modicum of effort. Citizens with technical knowledge can generally circumvent any filters that a state has put in place. Some states acknowledge as much: the overseer of Saudi Arabia's filtering program admits that technically savvy users simply cannot be stopped from accessing blocked content.[11] While no state will ultimately win the game of cat-and-mouse with those citizens who are resourceful and dedicated enough to employ circumvention measures, many users will never do so.

For some states, like Singapore, the state's bark is worse than the bite of the filtering system. The widely publicized Singaporean filtering system blocks only a small handful of pornographic sites. The Singapore system is more about sending a message, one that underscores the substantial local self-censorship that takes place there, than it is about blocking citizens from accessing or publishing anything specific. For other states, like those with the most thorough and sophisticated filtering regimes—for instance, China, Iran, and Uzbekistan—the undertaking is far more substantial and has far-reaching consequences.

Locus of Filtering

Most state-mandated filtering is effected by private ISPs that offer Internet access to citizens under licenses to operate in that jurisdiction. These licenses tend to include requirements, explicit or implicit in nature, that the ISPs implement filtering at the behest of the state. Some states partially centralize the filtering operation at private Internet exchange points (IXPs)—topological crossroads for network traffic—or through explicit state-run clearing points established to serve as gatekeepers for Internet traffic. Some states implement filtering at public Internet access points, such as the computers found within cybercafés or in public libraries and schools, as in the United States. Such filtering can take the form of software used in many American libraries and schools for filtering purposes, or *normative* filtering—government-encouraged social pressure by shop proprietors, librarians, and others as citizens surf the Internet in common public places.

The exercise of traditional state powers can have a powerful impact on Internet usage without rendering all content in a particular category inaccessible. China, Vietnam, and Iran, among others, have each jailed ''cyber-dissidents.''[12] Against this backdrop, the blocking of Web pages may be intended to deliver a message to users that the government monitors Internet usage. This message is reinforced by methods allowing information to be gathered

about what sites a particular user has visited after the fact, such as the requirement that a user provide passport information to set up an account with an ISP and tighter controls of users at cybercafés, as in Vietnam. The on-again, off-again blocking of Wikipedia in China might well be explained, in part, by this mode of sending a message that the state is watching in order to prompt self-censorship online.

While our research can tell us what Web sites a regime has targeted for filtering, the real extent to which the information environment is ''free'' and ''open'' is sharply limited. It is not as easy to determine, for instance, the extent of citizens' attempts to reach blocked sites, the degree to which citizens are deterred by the threat of arrest or detection, and how much the invisibility of specific content actually affects the regime's internal dialogue. Our research provides the data to draw conclusions about the choices made by states as to the content to be filtered, how these decisions are affected by the mechanisms for filtering they have employed, and how these governments attempt to balance the overblocking or underblocking that is today inherent in any filtering regime.

Types of Content Filtered

As Faris and Villeneuve describe in chapter 1, states around the world are blocking access to Internet content for its political, religious, and social connotations. Sensitivities related to specific content within these broad categories vary greatly from state to state, tracking, to large extent, local conflicts. The Internet content blocked for social reasons—commonly pornography, information about gay and lesbian issues, and information about sex education—is more likely to be the same across countries than the political and religious information to which access is blocked.

Web content is constantly changing, of course, and no state we have studied in the past five years seems able to carry out its Web filtering in a comprehensive manner—at least not through technical means. In other words, no state has been able to consistently block access to a range of sites meeting specified criteria. The most thorough job of blocking might be the high rate of blocking online pornography in Saudi Arabia and other Gulf states—a fairly stunning achievement given the amount of pornographic material available online—and one managed with the ongoing help of a U.S. firm, Secure Computing, that also assists schools in keeping children away from such Web sites. China has the most consistent record of responding to the shifting content of the Web, likely reflecting a devotion of the most resources to the filtering enterprise. Our research shows changes among sites blocked over time in some states, such as Iran, Saudi Arabia, and China. As we repeat this global survey in future years, we expect to be able to describe changes over time with greater certainty.

The Reality and Perception of Internet Surveillance and Other Soft Controls

Just as these several dozen states use technical means to block citizens from accessing content on the Internet, each state also employs legal and other ''soft'' means of control. Most

states use a combination of media, telecommunications, national security, and Internet-specific laws and regulatory schemes to restrict the publication of and access to information on the Internet. Most states that filter require Internet service providers to obtain licenses before providing Internet access to citizens. Some states place pressure on cybercafés and ISPs to monitor Internet usage by their customers. With the exception of a few places, no state seems to communicate much at all with the public about its process for blocking and unblocking content on the Internet. Most states, instead, have only a series of broad laws that cover content issues online. The effect of these regimes is to put citizens on notice that they should not publish or access content online that violates certain norms and to create a sense that someone might be paying attention to their online activity.

Our global survey of Internet filtering in 2006 turned up instances where the Internet is not subject to online filtering, but where the state manages to dampen online dissidence through other means. In Egypt, for instance, the Internet is not filtered (reports suggest that Egypt at one time blocked the Muslim Brotherhood site, but did not appear to do so during our testing),[13] but security forces have detained people for their activities online.[14] The perception that the online space is subject to extensive state surveillance leads to a broad fear of accessing or publishing information online that may be perceived to be subversive—though bloggers and other online activists cross the perceived lines with regularity.[15]

The Spectrum from Manual to Automatic Filtering

Most of the filtering regimes we studied, with the exception of parts of the Chinese filtering regime, appear to rely on the preidentification and categorization of undesirable Web sites. As the Web grows in scope as well as form, it is likely that states with an interest in filtering will attempt to develop or obtain technology to automatically review or generalize about the content of a Web page as it is accessed, or other Internet communication as it happens. The Web 2.0 phenomenon only makes this challenge harder, as citizens have the ability to publish online content on the fly and to syndicate that content for free.

The job of the censor in a Web 2.0 world might or might not be accomplished by looking for certain keywords in the title of the page or on its *link*—its URL. While URLs are clearly not as determinative of content as the name of a television channel or a newspaper, they may be in some situations (consider what generalizations one might draw about a URL of www.google.com/search?q=tiananmen). In others, a URL may serve as an adequate proxy—URLs containing particular obscene words are more likely to have obscene content. If the goal is to block all content coming from a particular state, the top-level domain structure makes this remarkably simple. On the other end of the spectrum, however, are blogging sites or generic free Web-hosting sites like www.geocities.com, where the presence of a page within the general site provides little information about the content or authorship of other pages on the site.

Despite the obvious imperfections of filtering via URLs, we have found little evidence that the states in which we tested, with the exception of China, attempted a dynamic assessment

of the content of a Web page instead of the URL at the time of request by a user. China may be the sole exception to this rule. Our research has documented an elaborate network of controls including keyword-based URL filtering; it may be the case that Chinese filtering systems can be triggered based upon the presence of keywords within a Web page's content. OpenNet Initiative researcher Steven Murdoch along with his colleagues Richard Clayton and Robert N. M. Watson have published a paper that describes in detail the workings of the ''Great Firewall of China,'' including this dynamic filtering based on Web page content. As Clayton, Murdoch, and Watson note, ''We have demonstrated that the 'Great Firewall of China' relies on inspecting packets for specific content.''[16] Yemen and Iran also have the capacity to block sites based on keywords in URLs. Commercial software packages such as SmartFilter make such URL filtering trivial. As a general rule, with the possible exception of China, access to a site is based on its URL; if a URL has triggered a block, one could take down the offensive content within the page and replace it with the most innocuous material possible, and the original link will continue to trigger a block.

URL-based blocking does not, however, require the identification of every page that is to be blocked. Our research indicates that the most prevalent form of blocking is at the domain level. Once a state has identified www.playboy.com as undesirable, the logical step is to deny all requests to that domain, whether http://playboy.com/playmates/2003/may.html or playboy.com/articles/interviews/index.html.

The parallel between the URL-based approach with the approach of the traditional censor is that the domain is deemed on the whole undesirable, and the censor makes no effort to disaggregate the content within. The decision is most complicated when a single domain hosts truly disparate content, such as free hosting sites like Geocities or Angelfire, blogging domains like Blogspot or Blogger, community sites like Google or Yahoo! groups, or university sites like mit.edu that can include student home pages about subjects like Tibet. Within these realms, our research found ample evidence of both blocking of the entire domain and selected blocking of *subsites*, or pages within the domain. Such blocking is discussed in the respective state reports in the appendix to this book. The Berkman Center's Web site at http://cyber.law.harvard.edu was blocked in China in 2002 after our first report of Internet filtering was placed there. (The powers that be in Harvard's central university administration declined to repost the study at www.harvard.edu.)

We have also observed several other means of URL-based filtering. As the results presented in chapter 1 show, several states—including China, Iran, Myanmar, and Yemen—block access to all URLs containing particular strings of letters (such as ''ass''), whether such banned terms appear in the domain or in superfluous characters at its end. Those sites' IP addresses are independently blocked, as blocked domains could otherwise be accessed via this method.

Some blocking approaches are cruder still. We observed that the United Arab Emirates and Syria blocked every site found within the Israeli top-level country code domain: no pages from any domain ending in ''.il'' were accessible there.[17]

This last example demonstrates the dramatic difference between URL-based filtering and content-based filtering. The structure of the Internet makes it very easy to block all sites ending in .il, but extremely hard, if not impossible, to block all sites containing content about Israel, a project that our data indicates was never seriously undertaken within the country. It may be that the purpose of blocking ''.il'' was more a statement about the Syrian and UAE view on Israel, rather than an attempt to prevent its citizens from discovering particular information. Also, the block likely operates in both directions: someone from a ''.il'' address may have a hard time accessing content in the UAE as a result of the filtering there.

The Role of Commercial Software in State-Mandated Internet Filtering

Commercial services, including the U.S.-based Secure Computing's SmartFilter, Websense, and Fortinet, appear to assist, or to have assisted, states that filter with the implementation and management of block lists. These services provide extensive lists of URLs categorized using proprietary methods. The commercial services typically fall in the middle of a spectrum between manual and automated filtering. The URL for a site found to contain content related to gambling will be offered as a digital update to the ''gambling'' block list of those states subscribing to the filtering services' lists.

For topics such as pornography or drugs, few states appear to invest the resources required to maintain active block lists where they can procure a list from commercial Internet filtering companies. The challenge in doing so is compounded by multiple means of typically accessing such Web sites—http://www.norml.com, http://norml.com, http://www.norml.org, and http://209.70.46.40 all bring the user to the home page of the National Organization for the Reform of Marijuana Laws. Each of these means of accessing the site (and others) must be added to the block list in order to block citizens' access in a thorough manner. The task is further complicated when site operators realize that they are being filtered and attempt to evade simple filtering techniques by changing their URLs; for instance, Iran has blocked the site at www.pglo.org, but in a subsequent test, it had not blocked the same content on www.pglo1.org.[18] Additionally, since filtering on a national scale requires complex infrastructure, making sure that the same list of blocked sites is present on each machine performing the filtering, at either a centralized or ISP-specific level, is no simple task.

A state subscribing to such a service is limited to the categories made available by the commercial software providers. While generally useful for content targeted according to the common desires of parents, schools, and companies in the West (such as ''pornography,'' ''drugs,'' or ''dating''), these products also include broad categories such as ''religion'' and ''politics'' that are not fine-tuned enough to match state-specific goals. These categories will not, in the off-the-shelf version of the software, include filtering of content critical of Islam or opposing the government of Vietnam. To account for the generality of these categories, each

of the installations of filtering software we observed appears to allow a state to augment a commercial block list with its own URLs.

Aside from such fine tuning, however, states using commercial filtering services must choose between allowing or blocking all URLs within a category. For example, a previous version of the SmartFilter service provides the choice of blocking or allowing all URLs in the ''anonymizer/translator'' category. Even though a state may wish to block anonymizers in order to prevent circumvention, that same state may wish to preserve access to translators as a useful tool.[19] Language presents an additional problem, as all the commercial filtering software we observed is produced by American companies. The blocking in states using these commercial filters therefore tilts heavily toward evaluating—and in turn prompting blocks of—English-language sites. This tilt leans precisely the opposite way from the tilt of those states that develop their own blocking systems, which generally seek to block content in local languages more than content in foreign languages. In some of the states using commercial filtering software, we have observed heavy filtering of English language content in some categories, while the same content appeared to be freely available in the local language—likely the inverse of what the state was seeking to accomplish through its filtering regime.[20]

When commercial filtering software is in use, a given second-level domain—for instance, cnn.com—may include some sites that are blocked and other sites that are unblocked. Our testing of SmartFilter has determined that the software attempts a more exact match first, and in its absence falls back to categories assigned more generally to areas of a domain or the domain itself. For instance, SmartFilter categorizes the *Sports Illustrated* home page at sportsillustrated.cnn.com as ''sports.'' The default categorization for any Web page located within this site, as shown by the category SmartFilter assigns to a request for http://sportsillustrated.cnn.com/does_not_exist, will also be ''sports.'' However, the page for the most recent swimsuit edition, at http://sportsillustrated.cnn.com/features/2006_swimsuit, is categorized as ''provocative attire/mature.'' Thus, it appears that any Web page within the *Sports Illustrated* site will, logically enough, be assigned to the ''sports'' category whether or not SmartFilter has analyzed the content of the page, unless this default has been overridden with a page-specific categorization.[21]

Commercial filtering software may alleviate some of the difficulties of filtering presented by the technical structure of the Internet. Our data show that states using such software are much less likely to miss alternative means of accessing blocked sites, for instance, visiting http://ifex.org to get around a block of http://www.ifex.org, as was possible in Vietnam during our testing. Commercial software companies have refined their filtering techniques to anticipate, detect, and prevent these relatively simple methods of evading blocking. There are others, as Deibert and Rohozinski note in chapter 6 of this volume, who seek to achieve just the opposite. A game of cat and mouse is well underway.

Filtering and Transparency

As Faris and Villeneuve document in chapter 1 of this book, states adopt a range of practices in terms of how explicitly they discuss their filtering regime with the public and the amount that citizens can learn about it. No state that we have studied in the past five years makes its block list generally available, though partial information has found its way to the surface in a few instances. In India, through freedom of information filings, some citizens have obtained information as to the list of those sites filtered. In Bahrain, citizens have compiled a partial block list and posted it to the Internet. In Thailand, prior to the 2006 coup, a list of many thousand Web sites had been posted online, plausibly leaked by the state, but not mapping closely to the facts we have observed. A combination of citizen efforts and the circulation of Pakistan Telecommunication Authority blocking orders on the Internet have resulted in a partial list of blocked sites in Pakistan coming to our attention.[22]

Saudi Arabia is the most transparent state in terms of Internet filtering. The Saudi state sets forth the rationale and practices related to filtering on an easily accessible Web site in both Arabic and English. (In our first round of testing, in 2002, Saudi Arabia enabled us to run tests directly against its system, but would not show us the list that it was using to determine which sites it was blocking at any given moment; since publication of our first report on this topic, the Saudis have disallowed us such easy and direct access to their system.) In Saudi Arabia, citizens may suggest sites for blocking or for unblocking, in either Arabic or English, via a public Web site. Access to most of these sites prompts a blockpage to appear, indicating to those seeking access to a Web site that they have reached a disallowed site. Most states have enacted laws that support the filtering regime and provide citizens with some context for why and how it is occurring, though rarely with any degree of precision. However, among the states we studied, some of the central Asian states that practice just-in-time filtering on sensitive topics—as well as China, whose officials sometimes deny the presence of Internet filtering—obscure the nature and extent of their filtering regimes to the greatest extent.[23]

Some states, such as Saudi Arabia and UAE, make an effort to suggest that their citizens are largely in support of the filtering regime, particularly when it comes to blocking access to pornographic material. For instance, the agency responsible for both Internet access and filtering in Saudi Arabia conducted a user study in 1999 and reported that 45 percent of respondents thought ''too much'' was blocked, 41 percent thought the amount blocked was ''reasonable,'' and 14 percent found it ''not enough.''[24] We have not delved into the veracity of these findings.

Citizens may, in some instances, participate in the decision making as to whether a site may be filtered or not. Three of the states in which we tested (Saudi Arabia, UAE, and Yemen) respond to a request for a blocked site with a page that includes a mechanism for suggesting that the particular URL may be blocked in error. However, to make such a suggestion requires the user to have knowledge of the content of the Web page not able to be visited—and the

confidence, perhaps not well-placed, that such self-identification would not put the user in jeopardy of state sanction.

Trends in Internet Filtering

Researchers associated with the OpenNet Initiative have been collecting empirical data on Internet filtering since 2001. Our methodology circa 2006 is far more sophisticated than it has been in the past. The coverage of our research is far broader, now covering every state known or credibly suspected to carry out Internet filtering. During this five-year period, we have observed the following trends:

- The overall trend in Internet filtering is toward more states adopting filtering regimes. The states with the most extensive filtering practices fall primarily in three regions: east Asia, the Middle East and North Africa, and central Asia. State-mandated, technical filtering does occur in other parts of the world, but in a more limited fashion, such as the Internet filtering common in libraries and schools in the United States, child pornography filtering systems in northern Europe, and the filtering of Nazi paraphernalia and Holocaust denial sites in France and Germany.
- Some of the newest filtering regimes, such as those coming online in the Commonwealth of Independent States (CIS), appear to be more sophisticated than the first-generation systems still in place in some states. The early means of filtering—such as Saudi Arabia's early system, with a heavy emphasis on pornography and offering citizens a clear blockpage—are no longer the only ways to accomplish Internet filtering. The net result is greater variation in what it means to filter content online.
- In the Commonwealth of Independent States and in parts of the Middle East and North Africa, the filtering we are seeing is highly targeted in nature and carried out ''just-in-time'' to block access to information during sensitive time periods. ONI principal investigator Rafal Rohozinski and his coauthor Deirdre Collings predicted such an eventuality: ''In democratically-challenged countries, we are likely to see increasing constraints on the 'openness' of the Internet during election periods, and these constraints may be more subtle than outright filtering and blocking.''[25]

  The ONI has monitored three elections to date, one in Kyrgyzstan (2005), one in Belarus (2006), and one in Nigeria (2007). As Rohozinski and Collings wrote,

  > The February 2005 elections in Kyrgyzstan marked the ONI's first foray into election monitoring. During the Kyrgyz elections ONI researchers were able to document two major Denial of Service (DoS) attacks directed against ISPs hosting major opposition newspapers. The attacks were commissioned from a commercial ''bot herder'' and traced back to a group of Ukrainian hackers-for-hire. ONI was not able to identify who was ultimately responsible for these attacks. Direct links to the Kyrgyz authorities could not be established. Thus, while no direct filtering took place, the DoS attack resulted in the indirect censorship of websites while exonerating the Kyrgyz authorities of any direct responsibility. The Kyrgyz case also raised the issue of who benefits most from this kind of indirect filtering. In Kyrgyzstan, the target of the DoS attacks—opposition

newspaper websites—continued to publish print editions while claiming that they were being ''censored'' by the government.

Of the Belarus election, Rohozinski and Collings wrote,

> [T]he quality and consistency of access to some sites varied considerably, and on critical days, up to 37 opposition and independent sites across 25 different ISPs were inaccessible from within the state-owned Beltelecom network. On election day and after the website of the main opposition candidate (Aleksandr Milinkevich) was ''dead,'' as was another opposition site—Charter 97. On the day that the police cleared the last remaining protesters from October Square (25 March) Internet connectivity by way of Minsk telephone dial-up services failed.
>
> And, there were three instances of confirmed ''odd DNS errors'' affecting opposition websites. While no case yielded conclusive evidence of government inspired tampering, the pattern of failures as well as the fact that mostly opposition and independent media sites were affected, suggests that something other than chance was afoot.[26]

The just-in-time filtering phenomenon has reared its head in the Middle East region as well. Bahrain blocked several Web sites in the run-up to the country's parliamentary elections in 2006 and Yemen banned access to several media and local politics Web sites ahead of the country's 2006 presidential elections. Bahrain also briefly blocked access to Google Earth in 2006, citing security reasons. For about a month in 2006, Jordan blocked access to the VoIP Web site skype.com, also citing security concerns.

- Our most recent data, collected in 2006 and 2007, suggest that we may also be seeing, for the first time, the emergence of in-stream filtering. This process involves entities based in large states—possibly including Chinese, Russian, and Indian ISPs—that provide Internet service to other states, passing along the filtering practices to their customer states. While the data are inconclusive that such in-stream filtering is taking place extensively, the hallmarks of such activity are present in our recent findings. We will continue to monitor closely for the emergence of this phenomenon, as it might point to a new series of security concerns.
- There is a continued growth in the creation of online information by citizens, including citizen journalism, in many parts of the world, but filtering is having an impact on how people carry it out. In some cases, the existence of a filtering regime leads these citizen journalists to limit the topics that they cover. For instance, environmental activists writing online in China have tended to stick closely to the issues related to the environment, which tend not to be blocked, while steering clear of related political topics that are censored. In other cases, such as the Middle East region, citizens banter with the censors. In the Commonwealth of Independent States we may be witnessing a backlash, in the form of Internet filtering, because of the perceived influence of citizen media on the outcome of elections there.[27]
- Citizens and citizen journalists practice self-censorship. For example, moderators of online discussion forums remove contributions that could lead to the blocking of the forums. On the other hand, cyberactivists exploit alternative technologies to circumvent filtering systems. Many Web sites that discuss sensitive issues use online groups such as Yahoo! Groups as part of their contingency plans, so once a Web site is blocked, users continue the discussion and the exchange of content via the group e-mails.

- We have evidence of more filtering at the edges than in a centralized manner, especially in the Commonwealth of Independent States. One might also consider the cybercafé-based controls in China, say, as compared to the approach of setting up the ''Great Firewall'' at the state's geopolitical boundaries. Those states that have not developed centralized filtering systems may find it more effective to build them at the edges. This phenomenon suggests that those who lobby against network blockages may have to expand their view of the network to include the devices that attach to it.
- We have observed an increase in alternative modes of filtering, both in engineering technique and through increased licensing, registration, and reporting requirements in some states.
- We have uncovered evidence of filtering undertaken by some Internet sites depending on where they believe their users to be located. In these instances, the entity that is publishing the sites—rather than the state where the person accessing or publishing the information is located—is limiting who can access its site. This process, combined with geolocation of the source of a request for a Web page, has occasionally been prompted in the past by a legal proceeding, such as the French insistence that Yahoo! not provide its citizens with access to certain Nazi-related items in the Yahoo! auction sites. More recently, our data show that gambling sites, U.S. military Web sites in the ''.mil'' domain, and some dating sites are filtered from the server side.
- States continue to be most concerned with blocking of sites in the local language, as opposed to sites in nonlocal languages—even though commercial filtering software sometimes accomplishes the inverse. In the Commonwealth of Independent States, blocking is almost exclusively of local-language sites. In the Middle East and North Africa, much of the blocking focuses on local-language sites, with some blockage of English sites—especially where commercial filtering systems developed in the United States are in use.
- Internet filtering is increasingly being used to block access to certain online applications beyond Web sites accessed by Web browsers. This trend is particularly important as software transitions toward more and more of an online service model. Google Earth and Skype, among other Voice-over Internet Protocol services, are blocked in some states. Other online applications, such as non-Web-based anonymizers that allow anonymous Internet usage, are consistently blocked in many places.

Normative Analysis of Internet Filtering

Few would condemn all those who would seek to filter Internet content; in fact, nearly every society filters Internet content in one way or another. Certainly all states regulate the information environment in some fashion, as Jack Goldsmith and Tim Wu's work makes plain.[28] The purpose of this research is to provide the empirical data needed to understand this form of state control online, what it means for the future of the Internet, and what choices are involved in a state's decision to filter the Internet.

The perspective in support of state-mandated Internet filtering is straightforward. States have the sovereign right to carry out Internet filtering as they see fit. The same goes for

Internet-based surveillance. Internet filtering and surveillance, this argument goes, is no more a matter for international decision making than any other domestic policy concern. The nature of the network and its potential uses are irrelevant to the analysis. The Internet is not exceptional.

There are several possible critiques of Internet filtering. First, one might argue that technical filtering is fatally flawed from the outset; because it cannot be carried out in a manner that is not over- or under-broad, it cannot be done in a way that is sufficiently protective of civil liberties. Second, as a related critique, Internet filtering implicates human rights concerns, particularly the freedom of expression, and extends to the freedom of association, of religion, and of privacy in some instantiations. Finally, one might conclude that Internet filtering is unwise on public policy grounds because it is anathema to the good things to which ICTs can give rise, such as innovation, creativity, and stronger democracies.

The hardest cases are those that some would argue are acts of law enforcement while others contend that they are clear violations of international norms. Consider a sovereign, jealous of the opposition's power, that disables access to opposition Web sites in the lead-up to an election—and then relents once the threat of losing control is abated—as some of our findings from central Asia would suggest happens. Or a state that routinely uses censorship and surveillance as a key element of a campaign to persecute a religious minority group. Or a state that relies upon online surveillance for the purpose of jailing political dissidents whose acts the state has committed to respect pursuant to international human rights norms. What about when a state is trying to protect public morals by keeping citizens from looking at garden-variety online pornography, but in so doing also block information on culturally sensitive matters, such as HIV/AIDS prevention or gay and lesbian outreach efforts? We set forth three primary critiques here. These cases, each real, put the normative problem of Internet filtering into sharp relief.

The Argument in Favor of Internet Filtering: Legitimate State Control Online

The need for states to be able to exercise some measure of control online is broadly accepted. Likewise, states ought to be able to provide rights of action—ordinarily, the right to sue someone—to their citizens to enable them to seek redress for harms done in the online environment. Though one might disagree, these core presumptions are not challenged in this book. The easiest, perhaps most universal case is the common abhorrence of child pornography. Most societies share the view that imagery of children under a certain age in a sexually compromising position is unlawful to produce, possess, or distribute. The issue in the context of child pornography is less whether the state has the right to assert control over such material, but rather the most effective means of combating the problem it represents, and the problems to which it leads, without undercutting rights guaranteed to citizens. The prevention of online fraud or other crimes, often targeting the elderly or disadvantaged, likewise represents

a common purpose for some measure of state control of bits online. Some would argue that intellectual property protection represents yet another such example, though the merits of that proposition are hotly contested.

One of the key findings of our research is the extent to which states cannot do the job of content control alone, which in turn adds another layer of complexity to the analysis of Internet filtering as a public policy matter. Where the state cannot effectively carry out its mandate in these legitimate circumstances, the state reasonably turns to those best positioned to assert control of bits. Often, though not always, the state turns to Internet service providers of one flavor or another. The law enforcement officer, for instance, calls upon the lawyers representing ISPs to turn over information about users of the online service who are suspected of committing a common crime, such as online fraud. As criminals use the Internet in the course of wrongdoing, states need to be able to access the increasingly useful store of evidence collected online.

The strongest form of this argument is that online censorship and surveillance is a legitimate expression of the sovereign authority of states. As we have described, Saudi Arabia, which implements one of the most extensive and longest-running filtering regimes, did not introduce Internet access to its citizens until the state authorities were comfortable that they could do so in a manner that would not be averse to local morals or norms. In particular, the Saudi regime has concerned itself with blocking access to online pornography, which it has done with a startlingly high degree of effectiveness over the past five years—though the scope of its filtering has grown over time, now including more political information than when we first began testing there in 2002.

A state has a right to protect the morality of its citizens, the argument goes, and unfettered access to and use of the Internet undercuts public morality in myriad ways. Many regimes, including those in Western states (including the United States), have justified online surveillance of various sorts on the grounds of ordinary law enforcement activities, such as the prevention and enforcement of domestic criminal activity. Most recently, states have begun to justify online censorship and surveillance as a measure to counteract international terrorism. Put more simply, Internet filtering and surveillance, in an environment where the Internet is considered a form of territory alongside land or sea or air, are an expression of the unalterable right of a state to ensure its national security.

Counterarguments: The Infirmities of Technical Filtering

One of the enduring facts of technical filtering of the Internet is that no state has managed to implement a perfect system. The primary deficiency of any technical filtering system is that the censor must choose between two shortcomings: either the system suffers from overbreadth, that is, sites that are not meant to be filtered are filtered, or underbreadth, that is, not all sites meant to be filtered are filtered. In most instances, the filtering regime suffers from a

combination of these two deficiencies. Coupled with the extent to which savvy Internet users can evade the filtering regime, state authorities undertaking technical filtering know that they cannot succeed completely.

The public policy questions to which these problems give rise are many and complex. If a filtering regime cannot be implemented in an accurate manner, should it be undertaken at all? Under U.S. law, these shortcomings make any such system constitutionally suspect, if not outright infirm, but other legal systems would likely draw a different conclusion. Is overbreadth or underbreadth preferable in a filtering regime? States often respond by turning more and more to intermediaries—search engine providers, ISPs, cybercafé owners, and so forth—to make these decisions on the fly.

Filtering and Overbreadth Internet filtering is almost impossible to accomplish with any degree of precision. A country that is deciding to filter the Internet must make an ''overbroad'' or ''underbroad'' decision at the outset. The filtering regime will either block access to too much or too little Internet content. Very often, this decision is tied to whether the state opts to use a home-grown system or whether to adopt a commercial software product, such as SmartFilter or Websense, two products made in the United States and licensed to some states that filter the Internet. Bahrain, for instance, has opted for an underbroad solution for pornography; its ISPs appear to block access to a small and essentially fixed number of blacklisted sites. Bahrain may seek to indicate disapproval of access to pornographic material online, while actually blocking only token access to such material, much as Singapore does. United Arab Emirates, by contrast, seems to have made the opposite decision by attempting to block much more extensively in similar categories, thereby sweeping into its filtering basket a number of sites that appear to have innocuous content by any metric.

Most of the time, states make blocking determinations to cover a range of Web content, commonly grouped around a second-level domain name or the IP address of a Web service (such as www.un.org or 66.102.15.100), rather than based on the precise URL of a given Web page (such as www.un.org/womenwatch/), or a subset of content found on that page (such as a particular image or string of text). This approach means that the filtering process will often not distinguish between permissible and impermissible content so long as any impermissible content is deemed ''nearby'' from a network standpoint. In the case of the above example, the WomenWatch site was unavailable in Vietnam not because of the state attempts to block all sites relating to gender equality issues (judged by the availability of all other similar sites we tested), but because of a block placed on the entire www.un.org domain.

Because of this wholesale acceptance or rejection of a particular site—which may or may not correspond to a given speaker or related group of speakers—it becomes difficult to know exactly what speech was deemed unacceptable for citizens to access. Bahrain, a state in which we have found a handful of blocked sites, has blocked access to a discussion board at www.bahrainonline.org. The message board likely contains a combination of messages

that would be tolerated independently and those that are explicitly meant to be subject to filtering. Likewise, we found minimal blocking for internal political purposes in UAE, but the state did block a site that essentially acted as a catalog of criticism of the state. Our tests cannot determine whether it was the material covering human rights abuses or discussion of historical border disputes with Iran, but in as much as the discussion of these topics is taking place within a broad dissention-based site, the calculation we project onto the censor looks significantly different than that for a site with a different ratio of ''offensive'' to approved content.

For those states using commercial filtering software and update services to try to maintain a current list of blocked sites matching particular criteria, we have noted multiple instances where such software has mistaken sites containing gay and lesbian content for pornography. For instance, the site for the Log Cabin Republicans of Texas has been blocked by the United States–based SmartFilter as pornography, apparently the basis for its blocking by United Arab Emirates. Our research suggests that gay and lesbian content is itself often targeted for filtering; one might surmise that, even when it is not explicitly targeted, states that implement related filters are not overly concerned with its unavailability due to overbreadth.

As content changes increasingly quickly on the Web and generalizations become more difficult to make by URL or domain name—thanks in part to the rise of simpler, faster, and aggregated publishing tools such as Weblogging (blogging) services—accurate filtering is likely to get trickier for filtering regimes to address over time unless they want to take the step of banning nearly everything. For example, free Web-hosting domains tend to group an enormous array of changing content and thus provoke very different responses from state governments. In 2004, Saudi Arabia blocked every page we tested on http://freespace.virgin.net and www.erols.com.[29] However, our research indicated the www.erols.com sites had been only minimally blocked in 2002, and the http://freespace.virgin.net sites had been blocked in 2002, but accessible in 2003 before being reblocked in 2004. In all three tests, Saudi Arabia practiced URL blocking on www.geocities.com (possibly through SmartFilter categorization), blocking only 3 percent of more than one thousand sites tested in 2004. Vietnam blocked all sites we tested on the www.geocities.com and http://members.tripod.org domains.

Contrast this last example with Yahoo! Groups, which Vietnam appears to filter on a group-by-group basis. We found that the state blocks access to the pages of two groups discussing the Cao Dai religion in general, but our testers were able to access the page of a California Cao Dai youth group. Two factors may play a role in this decision. Groups may provide more ''benefit'' to the censor, due to their interactive nature, and thus implicate the social and possibly economic impacts of the Internet. Groups, too, may have a limited, albeit large, number of possibilities—a single group could, in theory be monitored at the group level where there is much more metadata about the content contained therein, whereas Geocities could be grouped by user, but a particular user may offer large numbers of pages on very varied topics.

In our 2005 testing, we located 115 Weblogs within 3 large blogging domains (blogsky, blogspot, and persianblog) that were blocked in Iran. This blocking corresponded to only 24 percent of all blogs tested within those domains, and our testing was designed to locate blocked sites. Clearly, Iran desires to block access to some blogs, but has not seen fit to block all blogs. Our empirical data do not help to explain why filtering authorities in Iran made this decision, but it clearly was the result of a deliberate action. Also note that the site for www.movabletype.org, an application designed to allow blogging to take place on any domain, was blocked. Perhaps this indicates a policy of containing the blogs by restricting them to the large blogging domains, where they can then be reviewed and potentially filtered on a one-by-one basis.

China's response to the same problem provides an instructive contrast. When China became worried about bloggers the state shut down the main blogging domains for a period of weeks—much as they have, periodically, for Wikipedia. When the domains came back online, they contained filters that would reject posts containing particular keywords.[30] In effect, China moved to a content-based filtering system, but determined that the best place for such content evaluation was not the point of Web page access but the point of publication, and possessed the authority to force these filters on the downstream application provider. Most of these providers coded these restrictions into the software provided to bloggers. This approach is similar to that taken with Google to respond to the accessibility of disfavored content via Google's caching function. Google was blocked in China until a mechanism was put in place to prevent cache access.[31] In the fall of 2005, Saudi Arabia was reported to have blocked access to all blogs on the Blogger network, which plainly represented an overbroad set of blocks. These examples make clear the length to which regimes can go to preserve ''good'' access instead of simply blocking an entire service.

Alternate approaches that demand a finer-grained means of filtering, such as the use of automated keywords to identify and expunge sensitive information on the fly, or greater manual involvement in choosing individual Web pages to be filtered, are possible so long as a state is willing to invest the time and resources necessary to render them effective. China in particular appears to be prepared to make such an investment, one mirrored by choices made by the Chinese state in the context of traditional media. For example, China allows CNN to be broadcast within the country with a form of time delay so the feed can be temporarily turned off when, in one case, stories about the death of political reformer Zhao Ziyang were broadcast.

Filtering and Underbreadth One of the primary surprises in our data over the past several years is the infrequency with which plainly sensitive pages were blocked within otherwise acceptable sites. For instance, we found no cases where specific articles were blocked on major news sites, except in China. In fact, the regimes in which we tested very rarely made an attempt to block www.cnn.com, www.nytimes.com, http://bbc.co.uk, or others. (Exceptions to

this rule include the Voice of America news site at www.voanews.com. It was blocked in both Iran and China, and China also blocks the entire BBC news site.) In fact, not only was CNN's international news site at edition.cnn.com generally accessible in our China testing, a page within that domain dedicated to the massacre in Tiananmen Square was also not filtered. Several factors might be at work here—the sheer volume of news stories produced by major outlets may make thorough review impossible, or the speed at which new stories are posted may simply be too quick for an update across all the necessary filtering technology.

One instance where such URL-specific blocking had been applied in the past was Saudi Arabia's treatment of Amnesty International's Web site. In 2002, we tested twenty-five hundred pages within the amnesty.org domain and found nineteen blocked; all were within the directory www.amnesty.org/ailib/intcam/saudi, corresponding to a report entitled ''Saudi Arabia: A Secret State of Suffering.'' However, these same pages were tested in 2003, 2004, and 2006 and were accessible in each instance.

Human Rights Concerns Related to Internet Filtering

Internet censorship and surveillance prompt legitimate legal and normative concerns. Some state-mandated acts of online control are not straightforward acts of local law enforcement. As the practice of Internet filtering—and its close cousin, Internet surveillance—become more commonplace and more sophisticated, human rights activists and academics tracking this activity have begun to question whether some regimes of this sort violate international laws or norms. Quite often, the states that carry out online censorship and surveillance are signatories to international human rights convenants or have their own rules that preserve certain civil liberties for their citizens. The United States is home to a controversy of this sort as well, as the Electronic Frontier Foundation and others have filed a class-action lawsuit against telecommunications giant AT&T for collaborating with the National Security Agency in a wiretapping program.

The most straightforward of the critiques of Internet filtering and surveillance are grounded in concerns for individual civil liberties against the encroachment of overbearing states. The online environment is increasingly a venue in which personal data is stored. Personal communications increasingly flow across the wires and airwaves that compose the Internet. The basic rights of freedom of expression and individual privacy are threatened by the extension of state power, aided by private actors, into cyberspace. When public and private actors combine to restrict the publication of and access to online content, or to listen in on online conversations, the hackles of human rights activists are understandably raised. As Mary Rundle and Malcolm Birdling argue in chapter 4 of this book, one might contend that the right of free association is likewise violated by certain Internet-censorship and surveillance regimes that are emerging around the world. Most complaints cite the Universal Declaration of Human Rights or the International Covenant on Civil and Political Rights as grounding ideals—if not binding commitments—to which many states have agreed to hold themselves.

Concerns about Imposing Restrictions on the Internet

Even if one agrees with the strong form of the state sovereignty argument and sets aside objections based on international laws and norms, one might still contend that these filtering regimes are unwise from a public policy vantage point. Internet censorship and surveillance, the technologist might argue, violate the so-called end-to-end principle of network design and therefore risk stunting the future growth of the network and the innovation that might derive from it. This argument is typically grounded in adherence to the end-to-end principle. The end-to-end principle stands for the proposition that the ''intelligence'' in the network should not be placed in the middle of the network, but rather at the end-points. Technologists often chalk up the extraordinarily rapid growth of Internet throughout the world to this simple idea. By imposing control in the middle of the network—say, at the ''Great Firewall'' that surrounds China, proxy servers in Iran, or ISPs in dozens of states around the world—rather than at the user level, the censors are stymieing the further growth of the network.

The importance of ''generative'' information platforms also counsels against unwarranted state intrusion into the online environment.[32] Rather than hewing to the original design of the network, the decision-maker should favor those technical decisions that enable acts of innovation on top of the existing layers in the ecosystem—including not just the middle of the network, but also at the edges. The kinds of individual creativity made possible by the personal computer (PC), including self-expression in the form of the creation of user-generated content, might be thwarted by the presence of a censorship and surveillance regime. The on-again, off-again blockage of the user-generated encyclopedia, Wikipedia, makes this case clearly. The sporadic use of filtering regimes to block the use of Voice-over Internet Protocol (VoIP), often to protect the monopoly in voice communications of a local incumbent, also stands for this proposition.

These filtering regimes, along with surveillance practices that often go hand in hand with them, pose a danger in terms of having an adverse impact on the emergence of democracies around the world. The Internet has an increasing amount to do with the shape that democracies are taking in many developing states. As Ronald Deibert and Rafal Rohozinski argue in chapter 6 of this book, activists make use of the Internet in ways that are having a substantial impact on their societies.

The Internet is a potential force for democracy by increasing means of citizen participation in the regimes in which they live. The Internet is increasingly a way to let sunlight fall upon the actions of those in power—and providing an effective disinfectant in the process. The Internet can give a megaphone to activists and to dissidents who can make their case to the public, either on the record or anonymously or pseudonymously. The Internet can help make new networks, within and across cultures, can be an important productivity tool for otherwise underfunded activists, and can foster the development of new communities built around ideas. The Internet can open the information environment to voices other than the organs of the state that have traditionally had a monopoly on the broadcast of important stories and facts, which

in turn gives rise to what William Fisher refers to as ''semiotic democracy.''[33] Put another way, the Internet can place the control of cultural goods and the making of meaning in the hands of many rather than few. The Internet is increasingly an effective counterweight to the consolidation in big media, whether the Internet is controlled by a few capitalists or the state itself.

The Internet also can be a force for economic development, which is most likely the factor holding back some states from filtering the Internet more extensively or from imposing outright bans on related technologies. The Internet is widely recognized as a tool that is helping to lead to the development of technologically sophisticated, empowered middle classes. Entrepreneurship in the information technology sector can lead to innovation, the growth of new firms, and more jobs.

This critique of Internet filtering boils down to a belief in the value of a relatively open information environment because of the likelihood that it can lead to a beneficial combination of greater access to information, more transparency, better governance, and faster economic growth. The Internet, in this sense, is a generative network in human terms. In the hands of the populace at large, the Internet can give rise to a more empowered, productive citizenry.

An Alternate Viewpoint: The ''Slope of the Freedom Curve''

As our colleague Charles Nesson has pointed out, another vantage point altogether might lead to the best conclusion about Internet filtering. The point is not whether a single snapshot of an Internet filtering regime reveals a ''bad'' or a ''good'' system. Two jurisdictions, after all, could filter in exactly the same way, yet one could be moving toward freedom and the other toward further control of the online environment. In Professor Nesson's articulation, the issue is not the absolute extent of filtering at a given moment but rather the ''slope of the freedom curve'' that is most relevant. If the value at issue is whether an ICT environment is relatively open or relatively closed, then the key fact is whether a state is headed toward a more open system or a more closed system. The extent to which the Internet filtering picture is in constant flux lends further appeal to this vantage point.

Looking Ahead: The Future of Filtering, Weblogs, and Wikis

Regardless of whether states are right or wrong to mandate filtering and surveillance, the slope of the freedom curve favors not the censor but the citizens who wish to evade the state's control mechanisms. Most filtering regimes have been built on a presumption that the Internet is like the broadcast medium that predates it: each Web site is a ''channel,'' each Web user a ''viewer.'' Channels with sensitive content are ''turned off,'' or otherwise blocked, by authorities who wish to control the information environment. But the Internet is not a broadcast medium. As the Internet continues to grow in ways that are not like broadcast, filtering is becoming increasingly difficult to carry out effectively. The extent to which each person using the Internet can at once be a consumer and a creator is particularly vexing to the

broadcast-oriented censor. Combined with the absence of scarcity in terms of the number of channels or spectrum and the fast-dropping cost of accessing Internet from a wide range of devices including shared terminals and mobile devices, the changes in the online environment give an edge to the online publisher against the state's censor in the medium- to long-run.

Along with Wikipedia, Weblogs offer a poignant example of these growing challenges for the censor. No current filtering regime appears designed to address content developed on blogs, podcasts, and Wikis and accessed via Really Simple Syndication (RSS) feeds in aggregators, next-generation peer-to-peer networks, BitTorrent, and so forth. The most effective model demonstrated to date may be China's moves in the past few years to require blog service publishers to block keywords in blog posts, though even this approach can be only a partial means of blocking subversive content over time. Chinese bloggers routinely turn to broadly understood code words to evade the censorship built into the tools.

As online content changes very quickly and can be accessed through new means, the process of prescreening content and establishing a blockpage—akin to updating one's static virus definitions as new viruses are isolated and defined—breaks down. The process must become an heuristic one to function properly, if at all. Multimedia content, which is harder to screen and is accessed in different ways than through the World Wide Web, poses similar challenges for filtering regimes. Those states that are intent on filtering the Internet will have to adapt quickly if they intend to keep up. These adaptations might take the form of more aggressive filtering, or a shift to surveillance of user behavior with legal sanction for those who receive or transmit forbidden material.

In light of the prevalence of structural-based blocking in the states we studied, the trajectory of the Internet to a more dynamic environment will continue to create new problems for filtering regimes. The use of Weblogs by citizens—human rights activists, for instance—as a means of self-publishing is sharply on the rise in many cultures around the world. The general trend on the Internet is the divorcing of content from structure through the syndication of blogs via RSS and similar technologies. Syndication allows the text of a blog to be easily reproduced on other Web sites anywhere[34] in a way that circumvents filtering—since the retrieval of content from a blocked URL is done by the site the user is visiting, potentially located in a country with little or no filtering, instead of by the user's machine. While such mirroring of content has always been possible on the Internet, syndication represents a dramatic decrease in the amount of time and level of technical skill required to easily replicate content. In many ways, this freeing of content from structure mirrors how large sites are internally managed. The reason that CNN can easily display the same article at multiple URLs is that the text of the article can be retrieved from a single location, eliminating the need to separately create each HTML page on which it displays. Through this means, the acceptance or rejection of a large site in its entirety may in itself be a partial reaction to the problem created for URL-based structural filtering when content is not strictly tied to location.

Consider the implications for the censor of this technological change. The rise of publishing through blogs has caused concern in China, Iran, and Saudi Arabia at a minimum, judging from the reaction of their filtering regimes to block some blog-hosting services wholesale for a period of time. Assume that all blogs within the persianblog domain are available via RSS feed. The publisher could create a Web site specifically for the purpose of evading blocking, listing and displaying all such blocked blogs. This site itself could become a target for blocking by the Iranian government, since any mechanism for making this site known to users would also make it known to the filtering authorities.[35]

But using widely available aggregation tools, a user who wants to read this information does not need to go to a single URL to access the information published there. Instead, the user only needs to know the place where the XML feed is located at any given moment—which need not, ultimately, be at a stable location, so long as the user has a means of being updated as to its location at any given moment. In this version of the Web—trivial, using today's technologies—anyone can make any such blogs they choose available on any Web page or in an e-mail in-box or on a mobile device.

Another approach that citizen journalists might take would be to seek to bury the blocked blogs within a much larger number of blogs. The publisher could then establish a site or a feed that aggregates this larger number of blogs. Then, still using simple technologies, the readers could either read the full set of aggregated information or could run a filter of their own against the aggregated group of blogs to distill the information that the publisher wanted them to be able to access. Though these methods add a layer of complexity that would no doubt dissuage some Internet users, the net effect would be a publication mode that would be extremely difficult for the state to filter using current methods.

The state's censor would still have several options for responding to syndication methods of dissemination. First, the state could attempt to ban syndication, aggregation, and peer-to-peer technologies that might make these circumvention efforts easy to carry out. States have not, however, tended to pursue such a heavy-handed mode of regulation. Second, the state could seek to block the sites where the information is published and where the aggregation takes place. However, the potentially unlimited proliferation of such blogs and aggregator sites makes this unfeasible. A last option could involve a fallback to more traditional forms of state coercion—threatening both bloggers, readers, and those who provide them services with sanction. The difficulty of anonymous access leaves open the alternative of identifying users after they have accessed banned content. It is this last option that seems most in keeping with previous filtering and surveillance practices, especially since intermediaries closer to the user can be pressed into service to help.

The enduring point of this glimpse not so far into the future is that as Internet technologies continue to evolve, so too will state censors have to evolve their methods of Internet filtering if they wish to keep up. ONI's early election monitoring efforts in Kyrgyzstan and Belarus, combined with some of the most recent test results from the Commonwealth of Independent

States, suggest that some states are already seeking to turn on and off the Internet-filtering spigot at key moments. The simple proxy-based model, with a corresponding blockpage, will soon look as dated as a 1980s mainframe computer in a peer-to-peer world. If states persist in mandating filtering of the Internet, the narrative of China's on-again, off-again blocking of Wikipedia will be played out over and over as more citizens of the world build upon the generative Internet.

Notes

1. ''Wikipedia:Size comparisons,'' Wikipedia, http://en.wikipedia.org/wiki/Wikipedia:Size_comparisons (last accessed December 28, 2006).
2. ''Wikipedia:Overview FAQ,'' Wikipedia, http://en.wikipedia.org/wiki/Wikipedia:Overview_FAQ (last accessed December 28, 2006).
3. ''Blocking of Wikipedia in mainland China,'' Wikipedia, http://en.wikipedia.org/wiki/Blocking_of_Wikipedia_in_mainland_China (last accessed December 28, 2006).
4. *Ibid.*
5. See Jack L. Goldsmith and Tim Wu, *Who Controls the Internet: Illusions of a Borderless World*, (New York: Oxford University Press, 2006) 65–86; Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. Chi. L. Rev. 1199 (1998); Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 Ind. J. Global Legal Stud. 475 (1998); Jack Goldsmith and Timothy Wu, *Digital Borders*, Legal Affairs, Jan.–Feb. 2006, available at http://www.legalaffairs.org/issues/January-February-2006/feature_goldsmith_janfeb06.msp; Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. Rev. 653 (2003); Lawrence Lessig, *The Zones of Cyberspace*, 48 Stan. L. Rev. 1403 (1996).
6. ONI researcher Stephanie Wang deserves particular credit for her work on this taxonomy.
7. Consider the draft Cyber Crime Act, under consideration in the Kingdom of Thailand, on file with authors. Proposed section 14 would provide that ''service providers'' face criminal sanctions if they are aware of various offenses and ''do not manage to immediately erase such computer data.''
8. § 86 of the German Criminal Code. According to § 4(1) JMStV, online content involving the following is prohibited, irrespective of whether it is otherwise prohibited under criminal law or other law: 1) Propaganda against the democratic constitutional order (§ 86 of the Criminal Code). 2) Use of symbols of unconstitutional organizations (such as the swastika, § 86a of the Criminal Code) (an ''unconstitutional organization'' is essentially an organization that is against or threatens the principles of a free democratic state). 3) Incitement to hatred and violence against segments of the population or defamation of distinct groups. 4) Denial of the Holocaust or other specific acts perpetrated under the Nazi regime. 5) Depictions of cruel or inhuman violence against humans in a way that glamorizes such acts or makes light of their gravity—this includes virtual representations. 6) Depictions that instigate or incite the commission of certain crimes (namely, those defined in § 126(1) of the Criminal Code [Disturbance of the Peace through the Threat of Perpetrating Criminal Acts]). 7) Glorification of war. 8) Violation of human dignity through the depiction of human death or mortal suffering. 9) Erotic depictions of minors, including virtual depictions. 10) Pornography involving children, animals, or violence, including virtual depictions. 11) Content that has been blacklisted by the Federal Commission for Media Harmful to Young Persons or is similar in nature thereto. Translation and research assistance by Daniel Hausermann and James Thurman of the University of St. Gallen, Switzerland.
9. ''Why Block by IP Address?'' Internet Censorship Explorer, http://ice.citizenlab.org/index.php?p=78 (last accessed January 15, 2007).
10. For instance, IP filtering forces the choice of blocking all sites sharing an IP address. A recent ONI bulletin found over 3,000 Web sites blocked in an attempt to prevent access to only 31 (see http://www.opennetinitiative.net/bulletins/009/ [last accessed January 15, 2007]). DNS blocking requires an entire domain and all subdomains to be either wholly blocked or wholly unblocked (http://ice.citizenlab.org/index.php?p=78 [last accessed January 15, 2007]).

11. See ''Internet Filtering in Saudi Arabia in 2004,'' OpenNet Initiative, http://opennet.net/studies/saudi at n23 (stating the director of Saudi Arabia's Internet Services Unit director ''knows that anyone with much knowledge of the Internet and computers can blow right by the Saudi content filters'' and ''sees the filtering as a way to protect children and other innocents from Internet evils, and not much more than that'').
12. ''Appeal Court Confirms Prison for Cyber-Dissident While Blogger is Re-imprisoned,'' Iran: Reporters sans Frontières, http://www.rsf.org/article.php3?id_article=12564 (accessed February 15, 2005) (''Javad Tavaf, a student leader and the editor of the popular news website Rangin Kaman, which for a year had been criticising the Guide of the Islamic Revolution, was arrested at his home on 16 January 2003 by people who said they were from the military judiciary, which later denied it had arrested him.''). Internet—China, China: Reporters Sans Frontières, http://www.rsf.org/article.php3?id_article=10749. Internet—Vietnam, Vietnam: Reporters Sans Frontières, http://www.rsf.org/article.php3?id_article=10778.
13. See ''Blocking Web Sites,'' Human Rights Watch, http://hrw.org/reports/2005/mena1105/4.htm#_Toc119125716 (last accessed February 15, 2007).
14. See Elijah Zarwan, ''False Freedom: Online Censorship in the Middle East and North Africa,'' Human Rights Watch, http://hrw.org/reports/2005/mena1105/ (last accessed January 15, 2007). In addition to his work for HRW, Zarwan contributed research to the ONI work in 2006.
15. See Amnesty International, ''Egypt: New Concerns about Freedom of Expression,'' http://www.amnestyusa.org/news/document.do?id=ENGMDE120182006 (last accessed January 15, 2007).
16. Richard Clayton, Steven J. Murdoch, and Robert N. M. Watson, ''Ignoring the Great Firewall of China,'' http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf (last accessed January 15, 2007).
17. See, for instance, ''Syria,'' Human Rights Watch, http://hrw.org/reports/2005/mena1105/6.htm#_Toc119125750 (last accessed February 15, 2007), a report on Syrian blocking for which ONI provided technical testing support.
18. The effectiveness of such a maneuver will be limited by the need to publicize to users that the content can be found at the alternate site without bringing it to the attention of those managing the filtering.
19. This appears to have been the choice facing Saudi Arabia, where our research indicates that the category was generally allowed but the URLs for anonymizers were added to its local block list. Subsequent versions of SmartFilter have instituted separate categories for these two types of sites.
20. UAE has elected to block sites falling within the ''dating'' category, resulting in very high levels of blocking for English-language dating sites, but we found no blocking of Arabic-language dating sites.
21. The same default structure will also be applied to the ''2006_swimsuit'' directory: SmartFilter assigns the category of ''provocative attire/mature'' to a request for sportsillustrated.cnn.com/features/2006_swimsuit/does_not_exist. Again, the assignment of a default is always subject to a more granular categorization. We checked URL categorizations via the SmartFilterWhere tool at http://www.securecomputing.com/sfwhere (last accessed December 29, 2006).
22. See ''Internet Filtering in Pakistan,'' Internet Censorship Explorer, http://ice.citizenlab.org/?p=204 (last accessed February 15, 2007).
23. Chinese official Yang Xiaokun stated at the 2006 Internet Governance Forum (IGF): ''In China, we don't have software blocking Internet sites. Sometimes we have trouble accessing them. But that's a different problem. . . . We do not have restrictions at all.'' See transcript for October 31, 2006 ''Openness'' session, at http://www.intgovforum.org/IGF-Panel2-311006am.txt. The Uzbek government has also denied filtering, calling it ''impossible.'' See Ferghana.Ru news agency, ''Foreign Minister Eljer Ganiyev: We lack the capacities to restrict access to Internet,'' June 3, 2005, at http://enews.ferghana.ru/article.php?id=969; RadioFreeEurope/RadioLiberty, ''Rights Group Lists 'Enemies of Internet' at UN Summit,'' November 15, 2005, at http://www.rferl.org/featuresarticle/2005/11/2fdba63a-153a-4268-af4b-e6ebcf54e9ef.html (last accessed September January 3, 2007).
24. ''The Old User Survey Results,'' Internet Services Unit, http://www.isu.net.sa/surveys-&-statistics/user-survey.htm (last accessed September 7, 2004), reporting an online survey of 260 users from July through September 1999.
25. Rafal Rohozinski and Deirdre Collings, ''The Internet and Elections: The 2006 Presidential Election in Belarus (and its implications),'' OpenNet Initiative Internet Watch Report 001, April 2006, http://www.opennetinitiative.net/studies/belarus/ONI_Belarus_Country_Study.pdf (last accessed January 15, 2007).
26. Ibid.

27. See Regional Overview for the Middle East and North Africa and the Regional Overview for the Commonwealth of Independent States.
28. Goldsmith and Wu, *supra* note 5.
29. Except for the root page at http://www.erols.com itself, potentially indicating a desire to manage perceptions as to the extent of the blocking.
30. ''Filtering by Domestic Blog Providers in China,'' OpenNet Initiative, http://www.opennetinitiative.net/bulletins/008/ (last accessed January 15, 2007).
31. The mechanism for so doing turned out to be extremely rudimentary, as outlined in a previous ONI bulletin. See ''Google Search & Cache Filtering Behind China's Great Firewall,'' http://www.opennetinitiative.net/bulletins/006/ (last accessed January 15, 2007).
32. Jonathan L. Zittrain, *The Future of the Internet—and How to Stop It* (New Haven: Yale University Press, 2007).
33. William W. Fisher III, *Promises to Keep* (Stanford: Stanford University Press, 2004).
34. RSS also allows the user to access a blog via an application other than a Web browser such as a desktop aggregator. While we have not yet performed any testing in this area, it seems that a request issued directly to a blocked blog for an RSS feed would also be blocked, as it would be subject to the same filtering mechanisms despite the use of a different application. The RSS feed may be accessed at a different URL, but it stands to reason that, even if this were the case, the process of blocking a blog would simply be expanded to include this URL.
35. VOA has taken an interesting approach to a similar problem in its creation of a general anonymizer that fully circumvents government filtering. The site has a new address every day, which is broadcast via radio (and other means). ONI has not tested how quickly the Iranian filters are able to update and block these changing sites (see http://opennetinitiative.net/advisories/001/).