Censorship 2.0

volume 3 | issue 2 | spring 2008

A quarterly journal published by MIT Press

innovations

TECHNOLOGY | GOVERNANCE | GLOBALIZATION

Realizing Rights

ENTREPRENEURIAL SOLUTIONS TO GLOBAL CHALLENGES

innovations

TECHNOLOGY | GOVERNANCE | GLOBALIZATION

Lead Essays

Cases Authored by Innovators

Organization of the Journal

Each issue of *Innovations* consists of five sections:

1. Invited essay. An authoritative figure addresses an issue relating to innovation, emphasizing interactions between technology and governance in a global context.

2. Cases authored by innovators. Case narratives of innovations are authored either by, or in collaboration with, the innovators themselves. Each includes discussion of motivations, challenges, strategies, outcomes, and unintended consequences. Following each case narrative, we present commentary by an academic discussant. The discussant highlights the aspects of the innovation that are analytically most interesting, have the most significant implications for policy, and/or best illustrate reciprocal relationships between technology and governance.

3. Analysis. Accessible, policy-relevant research articles emphasize links between practice and policy—alternately, micro and macro scales of analysis. The development of meaningful indicators of the impact of innovations is an area of editorial emphasis.

4. Perspectives on policy. Analyses of innovations by large scale public actors—national governments and transnational organizations—address both success and failure of policy, informed by both empirical evidence and the experience of policy innovators. The development of improved modes of governance to facilitate and support innovations is an area of editorial focus.

5. Letters. Readers comment on essays and papers published in previous issues.

mitpressjournals.org/innovations
innovationsjournal.net

Robert Faris, Stephanie Wang, and John Palfrey

Censorship 2.0

The remarkable rise of social media has created a dilemma for countries determined to limit Internet content. With current technology, the standard methods of Internet filtering—blacklist and block—are not as effective at identifying and limiting content hosted via Web 2.0 applications, diminishing the impact of regulatory action of this sort within the jurisdiction of states.[1] In recognition of this, public-private transnational cooperation and coercion has been expanding to close gaps in the enforcement of state-mandated online content restrictions. These hybrid forms of filtering occupy gray zones of technological, political, legal, economic, and social policymaking and are fraught with contradictions and tensions.

A consequence of the internationalization of filtering is the growing demand for international solutions, many of which call for greater transparency where filtering occurs. However, the growth of social media amplifies the difficult balancing of interests implicit in the technical filtering of online content, between the effectiveness of regulation, the legal specificity of regulation, and the transparency by which regulation is enacted.

In this paper, we describe the regulatory approaches being developed in response to the emergence of social media, place evolving questions and policy issues in the context of prior efforts to regulate online content, and summarize the proposed international solutions. Without cooperation of the governments that are driving Internet filtering, legally compelling intermediaries to resist international filtering may prove to be counterproductive. Even demanding greater transparency—always worthy of protection—may have unintended negative consequences. Collective flexible approaches appear to be the more promising approaches at this pivotal time in the information wars between governments and their citizens.

Robert Faris is the research director, Stephanie Wang is a fellow and John Palfrey is executive director of the Berkman Center for Internet & Society at Harvard Law School. *This paper draws upon the work of the OpenNet Initiative (ONI), a four university consortium which joins the Universities of Cambridge, Harvard, Oxford, and Toronto, and with which the authors are affiliated. Prof. Palfrey is one of the principal investigators of the ONI, along with Prof. Ron Deibert at the Citizen Lab at the University of Toronto, Prof. Jonathan Zittrain of the Oxford Internet Institute, and Rafal Rohozinski of the University of Cambridge. The authors of this paper are grateful for the collaboration of their colleagues and are alone responsible for all errors and omissions.*

THE TOOLS OF DISSENT AND SOCIAL ACTIVISM

Although not new to the era of social media, the spread of ideas through communication technologies has played an important role in the politics and governance of nations. In turn, new communication technologies have also inspired and influenced the strategies governments use to suppress or disrupt the flow of information. At least since an office of censorship was created the 15th century following the invention of the Gutenberg press, advocates of free and independent speech and governments have tangled over the use of new communication technologies.

Dissidents and social commentators have consistently adopted and adapted to the technology of the times. For example, the printing press allowed pamphleteers writing about independence from Britain, such as Thomas Paine, to reach a relatively large audience at a politically charged historical moment. In France in the 1970s, speeches of the Ayatollah Ruhollah Khomeini were distributed as cassette tapes among the Iranian exile community, smuggled into Iran and widely distributed there, giving voice to the exiled religious leader and seeding the revolutionary sentiments that led to the overthrow of the Shah.

Since their inception, the Internet and mobile phone technologies have been central elements in the information wars between governments and their critics. Activists and organizers advocating on a broad range of issues, from democracy to women's rights and environmental issues, quickly adopted these digital tools. It is not unusual for governments to be slow to adapt to new technologies adopted by citizen groups and to be forced therefore to scramble to find ways to put the genie back in the bottle. Websites, weblogs, chat rooms, and text messaging were among the first digital tools used to promote independent expression and the spread of information previously controlled by governments or inhibited by the costs and reach of earlier channels of communication. In many of these countries, including countries with well-established systems of strict media control, such as China, Iran and Tunisia, bloggers offered their readers candid and alternative views of political and social events, with commentary and criticism from independent voices not found offline. The adoption of Internet tools, however, has not been uniform around the world; the citizens of other countries, such as Cuba, North Korea, and much of Sub-Saharan Africa, remain largely unconnected.

The political changes instigated by activists using these new communications tools are undeniable. A few notable events mark the beginning of the digital age of protest and mobilization. In the Philippines, activists gathered support for opposition rallies through text messaging that contributed to the large protests of 2001 resulting in President Estrada's resignation.[2] A second watershed event occurred in the Ukraine in 2004. Large scale protests against election fraud by the government of President Leonid Kuchma were organized using cell phones and website discussion boards. The events, later dubbed the Orange Revolution, led to new elections and helped sweep the opposition party into power.[3] In these two cases and many others, it is the expansion of the relatively low cost networks for spreading information that has proved to be the catalyst.

A number of prominent thinkers have noted how the spread of digital tools has triggered the devolution of power from traditional centralized institutions to the periphery, shifting the traditional balance of power, particularly in respect to the control and diffusion of information. Howard Rheingold's "smart mobs" are the embodiment of these large-scale mobilizations of citizens, whom he predicted would wrest a significant shift in the balance of political and social power.[4] Terry Fisher and others have highlighted the enhanced ability of citizens to shape the manner in which political and cultural events are debated, drawing on the concept of semiotic democracy first described by John Fiske.[5] In writing about the impact of digital networks, Yochai Benkler argues that citizens now have more power to contribute to the production of media, creating a media system that is more inclusive, democratic, and interactive than previous incarnations.[6] The potential of the Internet and mobile phones as tools for social and political change has not gone unnoticed by governments.

It is not unusual for governments to be slow to adapt to new technologies adopted by citizen groups and to be forced therefore to scramble to find ways to put the genie back in the bottle.

CONTROLLING INTERNET CONTENT

Efforts to control Internet content, which we will briefly summarize here, have been a prominent feature of the brief history of the Internet. These regulatory efforts provide precedents for current actions and context for understanding the choices and challenges of regulators now faced with the daunting task of regulating social media.

The feasibility, practicality, and wisdom of regulating Internet content have been subject to considerable debate. The mainly unregulated and rapid growth of the Internet in the 1990s helped to spawn cyber-utopian thinking among some, best exemplified by the often-cited Declaration of the Independence of Cyberspace, which was delivered to the World Economic Forum in Davos in 1996.[7] The opening lines capture the spirit of the manifesto:

> Governments of the Industrial World, you weary giants of flesh and steel,
> I come from Cyberspace, the new home of Mind. On behalf of the future,
> I ask you of the past to leave us alone. You are not welcome among us.
> You have no sovereignty where we gather.

The aspirations of many to maintain a self-governed domain separate from the restrictions of geographic nation-states did not, however, survive the test of time.

As documented by Jack Goldsmith and Tim Wu, governments have reasserted their sovereignty in cyberspace, reclaiming much of the ungoverned frontier.[8] Governments proceeded to do battle with illegal content on the Internet in ways largely consistent with the regulation of communications offline: passing legislation, identifying and prosecuting violators, and removing the offending content. This approach is reasonably effective on the Internet as well, except on the same frontiers where states have always been limited—with content produced overseas, out of the reach of domestic law. In the age of the Internet, geography and distance no longer limit the distribution of materials.

As documented by the OpenNet Initiative, well over three dozen states around the world use various mechanisms of Internet filtering, targeting a broad range of websites addressing political and social topics as well as many Internet tools and technologies.

Government regulators have found that they are able to block access to foreign-hosted content with the use of Internet filters. This practice, pioneered by China and Saudi Arabia, among other countries, has been proliferating in recent years. As documented by the OpenNet Initiative,[9] well over three dozen states around the world use various mechanisms of Internet filtering, targeting a broad range of websites addressing political and social topics as well as many Internet tools and technologies.

The concept of technical filtering is simple: compile a blacklist of banned websites and block access to these sites.[10] While the idealized architecture of the Internet is based on the end-to-end principle with little or no interference in-between, the actual architecture of the Internet includes "choke-points" that facilitate the implementation of filtering.[11] The most basic methods for Internet filtering—such as IP blocking—are trivial to apply. However, rudimentary filtering techniques typically result in either extensive over- or under-blocking, or both. More elaborate Internet filtering relies on both sophisticated software (to assemble and incorporate the blocking lists) and hardware (to filter Internet traffic). The most common manifestation of nation-wide filtering is initiated by a government entity (typically a court or executive agency) requiring Internet service providers (ISPs) within its jurisdiction to implement filtering of specific websites on the services that the ISPs offer to citizens of that state.[12]

PUBLIC-PRIVATE AND TRANSNATIONAL APPROACHES

The tendency of the Internet to untether the distribution of ideas from the con-

fines of geography has not only helped to spawn innovation but also provided a strong motivation for seeking transnational mechanisms for controlling content. The internationalization of Internet content control has been an important factor since the inception of filtering; the leading software and hardware providers have tended to be U.S. firms selling technology they claim to be value-neutral or positive, but which is used to suppress free expression in international markets. Certain of these companies have faced awkward or negative publicity when their products turned up in countries such as Burma, China, and Iran. In some cases, sales of these products would be not only difficult to explain but illegal.[13] These companies, however, are otherwise willing participants and profit from the sale of their filtering products.

A lawsuit filed in France opened a new chapter in the internationalization of content restrictions, challenging traditional conceptions of jurisdiction. In 2000, a Paris judge determined that Yahoo! Inc. was violating criminal law banning the exhibition or sale of racist material by providing French users with access to Nazi memorabilia on its auction site.[14] Some interpreted this as unleashing a scenario that, taken to its logical end, would subject any website to the laws of every jurisdiction. The court saw Yahoo!'s actions as infringing on French law in French territory. Yahoo! eventually agreed to block French users from sites that host material considered illegal in France through geolocational filtering, in which websites and web pages can be restricted to specific locations. Although less than perfect in pinpointing the location of users, this technique has contributed much to the growing balkanization of the Internet.

Though the court's ruling did not "smother the golden goose of e-commerce,"[15] a private company had been enlisted to enforce content restrictions for a foreign government. This is a far different process than the technological implementation of filters by a state within its borders, even if using foreign technologies. Many argued that an important and strong precedent was set in this case. Others dismissed the unique nature of the global Internet as a defining factor in what they perceived to be a natural extension of governments' responsibility to address harms felt locally but caused by a foreign source.[16]

ENLISTING INTERNATIONAL INTERMEDIARIES

The experience of Yahoo! with the French courts proved to a portent for further blocking requests. In 2002, researchers at Harvard Law School found that the French and German versions of the popular Google search engine were dropping certain websites from their search results, including hate speech and obscenity.[17] Figuratively speaking, the books were still on the shelves, but the librarian would not tell the patron their precise location. Although based on laws that clearly ban hate speech, the filtering of localized search engines was an informal bargain between Google and the German and French governments.

Unsurprisingly, China would desire concessions from Google similar to those granted to France and Germany. Google, which had ambitions to capture a healthy

portion of the expanding Chinese search market, found itself subject to frequent disruptions in access of its unfiltered flagship search site, Google.com, through degradations in speed and intermittent blocking. The message to Google was unmistakable: serious engagement in the Chinese search market would require filtering their search results to the standards of government regulators focused on maintaining their control over political information. This placed Google on potentially more treacherous footing as compared to its cooperation with France and Germany.

At the baseline, the number of websites to be de-indexed would be much greater and include sites that fell well within the bounds of protected speech in accordance with international human rights standards. Questions about the legitimacy of the Chinese government's controls on information notwithstanding, Google also became a participant in the purposefully informal system of censorship enforcement in China. China keeps its instructions and orders for filtering and prohibited content mostly informal and hidden from public view. In a quintessential act of self-censorship, while Google is given official guidance on what topics to remove from its search service, it has been charged to draw the line for itself in identifying and purging sensitive content.[18]

Within Google, there would be no easy consensus. Andrew McLaughlin, Google's senior policy counsel, writing on the Google blog explained at the time of the company's decision to enter the market, in January 2006:[19]

> Launching a Google domain that restricts information in any way isn't a step we took lightly. For several years, we've debated whether entering the Chinese market at this point in history could be consistent with our mission and values. Our executives have spent a lot of time in recent months talking with many people, ranging from those who applaud the Chinese government for its embrace of a market economy and its lifting of 400 million people out of poverty to those who disagree with many of the Chinese government's policies, but who wish the best for China and its people. We ultimately reached our decision by asking ourselves which course would most effectively further Google's mission to organize the world's information and make it universally useful and accessible. Or, put simply: how can we provide the greatest access to information to the greatest number of people?

The launch of Google.cn, a China-specific filtered search service, was a watershed event in the evolution of Internet content control. Ultimately, Google resorted to a solution that it considered to be thoroughly pragmatic and one that ultimately could increase access to information in China. The balancing of relevant factors in these decisions, from Google.de to Google.cn, was undoubtedly a complex process. They do not appear to have been made on the sole basis of compliance with local law or conditions mandated for market access, as determined users in all these countries can continue to access unfiltered results by simply using Google's pri-

mary search service, Google.com. Thus, the specific tailoring of search engines to operate along a spectrum where the richness and availability of information is compromised for the sake of national values or law. Regardless, at this juncture Google became committed to, if not entrenched in, what now appears to be a *de facto* policy of public-private negotiated transnational filtering at government behest.

In cooperating with the pressure from governments, Google is not alone. Microsoft and Yahoo! had fallen in line with similar restrictions being placed on their China services. For example, the search engine available to Yahoo! users within China is filtered to match government blocking criteria and Microsoft's MSN Spaces does not allow users to name blogs or write posts with certain sensitive keywords.

The launch of Google.cn, a China-specific filtered search service, was a watershed event in the evolution of Internet content control.

FACILITATING PRIVATE ACTION FOR COPYRIGHT PROTECTION IN THE U.S.

Efforts to curtail online copyright infringement have paralleled efforts to regulate sensitive political and social content and both have drawn upon similar technical, legal, and administrative approaches. The U.S. has crafted a strategy that relies heavily on private action to address the profusion of copyright issues on the Internet and the impracticalities of implementing monitoring of Internet content at such a large scale. In the U.S., the law facilitates private-private procedures that resolve a large majority of such cases without involving courts. The notice and take-down system is contingent on copyright holders communicating directly with intermediaries, such as hosting companies, and request the removal of infringing materials.

This too is a pragmatic solution, though one that leaves many questioning the underlying biases in the structure of the process. Hosting entities are criticized for being too quick to take down materials suspected of copyright infringement. Further, the notice and takedown system may contribute to an imbalance of power, allowing large corporations to intimidate smaller entities and content contributors with the threat of legal action, even where the legal basis for removing content is tenuous.[20] However, from a standpoint of regulatory efficiency, this system works well; relatively few instances require costly public intervention or private litigation.

THE RISE OF SOCIAL MEDIA

Just as many governments were settling into blacklist-and-block content filtering strategies, another revolution in the sharing of information was to complicate

these efforts: the rise of social media.[21] The growth of social media challenges current content control strategies. Compared to traditional media, social media thrives on a multitude of small producers, where the content is not defined by a relatively small number of professionals but through countless user contributions.

Technological innovation has again spurred social change—the tools for aggregating digital media have facilitated the culture and practice of sharing. The technological advances and falling cost of digital video recorders and cameras have helped to propel photo and video aggregation sites such as Flickr and YouTube.[22] Although the most prominent, YouTube is but one of many examples of this new model of content hosting.

Prior to the surge in user-generated content, government censors have had reasonable success in blocking access to specific websites that they deem to be inappropriate, offensive, or illegal. In Iran, Saudi Arabia, Tunisia, and the United Arab Emirates, all Internet traffic is routed through proxy servers that allow censors to block by the specific URL, removing content selectively and more accurately than the cruder methods found in other countries. China has adopted a unique and sophisticated system that combines at least three separate blocking techniques.[23]

Social media makes filtering more difficult not only because of the amount of content produced but also because of the multimedia formats commonly used in this production. With the rise of inexpensive video and audio production, the proportion of text in digital communication has dropped, with more images, videos and audio filling broadband connections. Earlier advances in indexing and searching text-based communications are not easily applied to multimedia platforms, complicating content control strategies.

Social activists have been quick to adopt these new communication technologies. One enterprising social critic in Bahrain made use of readily accessible Google Earth images to make a simple and powerful pictorial exposé of inequalities of landownership in Bahrain.[24] Google Earth was subsequently blocked in Bahrain for a few days after this incident.[25]

Facebook and other social networking sites have become important aggregation points for social causes. In a prominent example, a Facebook group, "A Million Voices against FARC," served as the node for organizing hundreds of protests in Colombia that brought several million people into the streets.[26]

The digital video revolution has struck even Cuba, a country in which Internet communications are controlled primarily by preventing citizens from getting online. A video recording of students confronting the president of the Cuban National Assembly, Ricardo Alarcon, can be found on YouTube and other video sharing sites.[27] In Cuba, these videos have circulated on USB flash drives for those with access to computers but without Internet access. The recording of such an exchange, as well as the exchange itself, are remarkable events in a country that has kept dissent in check so successfully and consistently.

NEW GATEKEEPERS

The remarkable success of social media sites has facilitated the entry of more individuals and small organizations into the media environment, adding to news coverage, commentary, arts, and entertainment. This success has also made the social media sites important new nodes in the architecture of information-sharing; the paradox of the increasing power of individual expression on the Internet is that it depends now in large part on aggregation points such as YouTube and Facebook. Moreover, housing vast amounts of content, such as videos, photos, podcasts, and blogposts, contributed by users, anonymous or not, produces pressure on these social media platforms to police content on their sites. Many of these challenges arise not only from government pressure or regulation. Rather, as principal conduits for information for millions of users, these new media companies must consider how to regulate user-submitted content in response to market forces, shareholder interests, and social values and ethical standards.

Whether faced with social, market, or regulatory pressures, social media companies face a complex set of choices related to the selective ban of certain types of content. Providing access to the most comprehensive set of available resources to Internet users is a good starting point. Facilitating the removal of illegal material, as determined by governments in the countries they operate, is a reasonable additional goal, or, in the case of search engines, not reporting the existence and location of these materials. However, the criteria for selecting operational principles for search engines and social media sites appear to be quite different, a contrast between providing a link to controversial content and actually hosting offensive content on one's servers. With the rise of social media, we have learned that the architecture for the sharing and distribution of multimedia content is providing a platform for incredibly reckless, violent, and thoughtless users. Social media sites have elected therefore to restrict content in ways that search engines have not. User agreements and terms of service agreements prohibit the posting of material that many might find highly offensive. The mostly commonly used model for moderating content on social media sites depends on user monitoring and reporting of offensive content, and is augmented by technical tools and company oversight.

This strategy appears to be a reasonably robust approach towards moderating content with a very large volume of submissions. The success of this strategy relies on the flexible implementation of general standards, with the companies as the ultimate arbiters of what is acceptable or not. However, a case-by-case review of the most difficult cases is also warranted, although time-consuming and thereby expensive. For example, YouTube suspended a user's account in the fall of 2007 for posting graphic video clips of torture. This user was Wael Abbas, a prominent Egyptian human rights activist and blogger documenting the excesses of the Egyptian police.[28] Citing a misunderstanding between Abbas and the company, YouTube reinstated his account following a strong outcry among rights activists. The complex calculus of determining how to balance conflicting objectives will remain—in this example, limiting exposure to graphic violence and reporting on

human rights abuses.

Although sexually explicit and violent materials are continually removed from YouTube and Flickr, this type of content monitoring system is neither designed nor easily adapted for the needs of government censors. Rather, this system is intended to suit the needs and sensibilities of the companies and their user communities. However, the norms that help to guide this process vary considerably across communities and countries, creating tension between standard global use policies of the site and local values. This raises the legitimate question of whether additional interventions are warranted to ensure that content is congruent with local values.

GOVERNMENTS ENTER THE FRAY OF SOCIAL MEDIA

It is no surprise that social media sites have become the next target for government content restrictions. Though not designed for this purpose, these sites have inadvertently become a channel for circumventing many of the most common control mechanisms. Images and videos documenting the protests and ensuing government crackdown in Burma in the fall of 2007 were distributed via blogs, aggregation sites, and dissident organizations and media outlets around the world. The digital recording and sharing of these events stand in sharp contrast to the protests of 1988, which were not so readily visible to the world. This undoubtedly contributed to the Burmese junta's decision to shut down the entire Internet in Burma for the better part of three weeks in the wake of the turmoil,[29] though significant damage to the official version of events had already been done.[30]

Technological capacity is a vital consideration in the evolution of filtering policy. For governments, the surge in multimedia file sharing on the Internet has made the prospect of controlling Internet content more complex. With the profusion of user-contributed posts, images, and videos, governments have no hope of keeping up with the production of content. Even software providers that have helped to carry out filtering functions are less capable of sorting through and categorizing the growing body of information and opinions. The net result is that the recent increase of user-generated content reduces the effectiveness of the blacklist-and-block model. While blacklist-and-block strategies for controlling Internet content will not become obsolete in the near future, these familiar tools must be complemented with newer, more sophisticated strategies to remain effective and if regulators hope to police social media.

In following the strategy taken with the major search engines, regulators are again looking to intermediaries to assist in restricting content. These intermediaries are most commonly the transnational technology companies, some of which are in fact the same companies that faced earlier pressure—YouTube is owned by Google and Flickr by Yahoo!. Major aggregation sites are enlisted as potentially powerful gatekeepers, joining ranks with government regulators, search engines, and ISPs. As with the ISPs before them, these social aggregators are now another focal point in the ongoing struggle over acceptable expression via the Internet.

Yet these new social media companies are not eager participants in limiting

content on their sites, particularly if this means negotiating such restrictions with dozens of regulators around the world. Their success is contingent upon providing content and continued access to global Internet markets, not in restricting users from content they would choose to view.

THE "BLOCK OR BE BLOCKED" DILEMMA AND PUBLIC-PRIVATE TRANSNATIONAL FILTERING

With the growing political salience of social media sites, governments' threats to blockade access to their markets has been an effective bargaining tool in pushing for increased censorship that spans international borders. Based on negotiations between foreign governments and private companies, this type of filtering is the latest manifestation of efforts being waged transnationally to enforce local content standards. However, in more recent instances it is not courts publicly deciding to pressure the private actors, as in the example of the Yahoo! case in France, but rather executive branches of governments using private requests to apply coercive pressure to enlist the cooperation of these companies. As we discuss later, transnational negotiations offer flexibility and the scope for pragmatic informal solutions, but at the cost of decreased transparency and reduced reliance on clearly articulated formal legal processes.

As the world's leading video-sharing website, YouTube has recently found itself embroiled in several difficult policy challenges that are reflective of the emerging conflicts and policy issues involved in policing "borderless" social media. The large amount of content available on YouTube, especially political satire and video footage of unfolding political events, makes it a target for blocking by governments who find themselves vulnerable to critique, mockery, and unwanted exposure.

Few countries have the capacity to block individual videos, and even where this is technically possible, it is infeasible in practical terms to keep apace with the volume of material being posted, and reposted if taken down. ISPs in many of the countries that are intent on blocking YouTube content, but do not have the capability to filter individual videos, have few choices: they can do nothing, block the entire YouTube site, or lean on Google to selectively block videos for them. More than a dozen countries have at times chosen the "nuclear" option, blocking the entire YouTube site in response to a relatively small number of undesirable video clips. Over the past two years, YouTube has been blocked in a wide number of countries, including Armenia, Brazil, Burma, China, Indonesia, Iran, Morocco, Pakistan, Syria, Thailand, Tunisia, Turkey, and the United Arab Emirates. In most of these cases, the blocking of YouTube has been intermittent, and in many instances, short-lived. Most of these countries are accustomed to strong oversight of traditional media and are struggling to achieve similar control over the Internet. For YouTube, it has become clear that they would not be ignored.

In April 2007, the Thai government moved to block a number of videos appearing on YouTube that had no apparent objective except to offend King Bhumibol Adulyadej of Thailand. In Thailand, insult to the King is not only in

poor taste, but constitutes *lese majeste*—the crime of defaming, insulting, or threatening the royal family. It is punishable by up to 15 years imprisonment.

YouTube's Terms of Use policy states that users may not submit material that is contrary to applicable local, national, and international laws and regulations.[31] At the time, YouTube did not believe that the removal of these videos insulting the King of Thailand was warranted, claiming it would not assist in implementing censorship for videos that did not violate its use policy.[32] However, YouTube did engage in a process of publicly tracked negotiations with the Thai government. By May 2007, YouTube had modified its position, removing a number of the cited videos for violating its user agreement.[33] The overall block was lifted in August 2007 upon Google's creation of a "program" of geolocational filtering that would only block access to these disputed videos for users in Thailand.[34]

The opposition to *lese majeste* is firmly grounded in Thai law and culture, though it is not a concept congruent with norms of free expression in the West. However, Google had already embarked along a slippery slope of participation (and some would say complicity) with censorship regimes, from Google.de to Google.cn. In this context, YouTube's initial refusal to cooperate with the Thai authorities appeared to be more of a clash of political and social sensibilities, opening it to criticism that it defended its market interests more than any discernible stand on promoting free expression. It is unclear whether the existence of democratic processes of governance in a given country factors into companies' decisions to accept delegated filtering responsibilities, or whether all government requests are considered presumptively legitimate.

It is not publicly known how many times Google has been pressed into this "block or be blocked" situation, though it is likely that there are many more incidents than those reported in the press. Were Google to adhere consistently to the explanation of its Google.cn policy, it could increase the net flow of information to YouTube users in these countries by selectively removing the relatively small number of videos that offend in certain countries, thereby preempting the more costly blocking of the entire site. Regardless, YouTube has been placed on this trajectory of public-private transnational efforts to achieve a "bordered Internet,"[35] one that would drive future negotiations with the government of Thailand as well as potentially dozens of countries around the world.

CODING FOR A FRACTURED INTERNET

Larry Lessig's iconic assertion, code is law, aptly describes an essential element of the institutions and infrastructure that govern expression on the Internet.[36] Software writers have wielded a strong influence on the accessibility of Internet content around the world, whether in designed filtering software or in configuring routers used for filtering. The decisions taken in the coding of social media websites will also make them more or less conducive to filtering.

Investigations by YouTomb, a project of the MIT Free Culture group, appear to have uncovered the code for a technical mechanism that YouTube uses to imple-

ment selective, geolocational filtering. YouTomb was formed to explore the development of automated means for detecting and identifying videos on YouTube that infringe on copyright.[37] In the course of their research, they found a tag appearing on a number of YouTube videos:

[**media:restriction type="country" relationship="deny">TH**]

In this example, the country code, TH, refers to Thailand. A video with this tag can be seen anywhere YouTube is available, except Thailand. The majority, but not all, of the videos leveling insult at the King tested by ONI and YouTomb carry the restriction flag. When trying to access these clips, users of the Thai ISP CAT see a pink band across the top of the YouTube page which states, "This video is not available in your country."

As demonstrated with the solution imposed by Yahoo! France in 2000, this geolocational filtering capability is not new. Businesses have long been leveraging this technology to target the presentation of materials, sales strategies, and advertising by region and language. It is also a useful device for companies to work with governments to abide by local law. For example, the accessibility of gambling sites can be tailored to its legality in various jurisdictions.

However, as a highly informal and nontransparent mechanism, the country restriction flag also introduces the risk of escalated transnational filtering across public-private lines. It provides a resonant example of how governments can negotiate censorship with private actors with scant public knowledge, oversight, or involvement. The flag can be easily scalable to block videos in many more countries in a process that remains largely opaque. This architecture, while itself value-neutral, can be as readily applied to illegitimate suppression of speech as it is to lawful ends. For example, in contrast to the private-private mechanisms of allowing users to flag videos for removal, there does not appear to be a way for ordinary users to code this country restriction flag.[38] The videos identified thus far to carry this country restriction flag suggest that certain private interests as well as government authorities have prevailed on YouTube to assist in regulating content.[39]

INTERNET FILTERING: TRANSPARENCY, EFFICACY, AND SPECIFICITY

The growing prominence of social media sites highlights the trade-offs inherent in implementing content filtering on a large scale and the tensions between efficacy, specificity, and transparency. Blocking of Internet content often lacks transparency and is frequently carried out without resort to formal legal procedures. When done surreptitiously, filtering is also arguably more effective in preventing citizens from accessing what their governments determine to be inappropriate material. Transparent government regulation that follows well-defined legal procedures is offset by reduced effectiveness in preventing users from being aware of and accessing sensitive content online. These competing tensions create policy challenges for governments that seek to limit online content in an era where social media platforms are ascendant, offering citizens greater opportunities for political participation. Transparent, legally formalized regulation that is also effective may be consid-

ered ideal. However, the continual growth in the amount of information on the Internet from international sources makes this infeasible using current technology.

Some recent examples associated with blocking access to Internet sites elucidate these trade-offs. In February 2008, a federal judge in the United States sought to block access to the website Wikileaks (http://www.wikileaks.org) after the Swiss bank Julius Baer filed suit against the website for publishing its leaked documents.[40] From a legal standpoint, the grounds for blocking the entire website were dubious. The blocking of the Wikileaks website would entail the removal of a great amount of material unrelated to the complaint.[41] Despite this and other serious problems with the original court order, the order was both specific and transparent, which many consider essential aspects of Internet regulatory decisions. It also proved to be highly ineffective, as mirrored versions of the website remained available throughout the period of enforced blocked.[42] After the ban was ultimately lifted, Judge Jeffrey White shared his realization that it is next to impossible to suppress information once released on the Internet. He remarked, "Maybe that's just the reality of the world that we live in. When this genie gets out of the bottle, that's it."[43]

In another example, the organization that represents the international recording industry, IFPI, convinced an Israeli ISP to block the website, www.httpshare.com. The block resulted in significantly higher traffic to the site, so much so that the site administrators had to upgrade their equipment in order to handle the additional traffic. In both of these examples, open attempts to censor the Internet proved to be unsuccessful. It is natural for the online public, once notified of an instance of Internet filtering, to drive more traffic to the targeted sites, which are easily moved and mirrored to multiple new sites if necessary to avoid blocking orders.

Many countries have grappled with the question of transparency in blocking decisions and few have chosen to adopt a high standard of transparency. The voluntary filtering systems in place in a number of European countries and Canada are designed to block access to child pornography. The blocking lists that they compile are not public. In Finland, an anti-censorship website that chose to publish the block list of so-called child pornography sites was subsequently filtered itself.[44] For governments, there is a natural logic in deciding to not publish lists that identify pornography. However, for those that seek to ban Internet content, the practical implications of making a blocking list public apply equally to any content category, whether pornography, copyright, or political speech; publication is at odds with the objective of inhibiting access and reducing traffic to these sites. Yet, without some measure of transparency, it is difficult to construct a system by which the blocking of sites can be assessed and debated by the public.

Turkey currently implements one of the most transparent filtering regimes. A Turkish cybercrimes law enacted in May 2007 allows for ISPs to seek court approval for blocking of content that insults Kamal Ataturk and incites suicide, drug use, and prostitution, and administrative discretion over blocking of child pornography and obscenity.[45] When it finds offense with videos on YouTube ridi-

culing Ataturk and other Turkish leaders, it relies on court orders to block all of YouTube until the content is removed from the site. The Turkish block page includes the name of the court and the case number.[46] To date it has blocked YouTube (several times), WordPress, and Google Groups.[47] However, the administrative and legal costs involved in this highly formal process make this filtering system less nimble. Turkey's method, in which millions of sites hosted on WordPress were blocked in response to a single defamation claim, also results in significant overblocking. On balance, this may levy a heavier collateral cost than YouTube's geolocational filtering of a select number of videos. Attempts to legally formalize processes to achieve complete transparency complicate the practicability, effectiveness, and costs of executing content restrictions. For societies that value transparency, there are no simple ways to filter the Internet effectively and comprehensively.

For societies that value transparency, there are no simple ways to filter the Internet effectively and comprehensively.

A more prevalent version of transparency is also less stringent—notifying users when they attempt to access a blocked website.[48] To their credit, Google informs users when the results of a search query have been filtered: "*A portion of these search results cannot be displayed in accordance with local laws and regulations.*" YouTube similarly discloses when a video is unavailable: "*This video is not available in your country.*" These notifications are better than no notification at all. However, they do not provide users information on the processes, negotiations, and concessions underlying the censorship. For search engines, the list of sites that are removed from search results—sites that are effectively made invisible to most users—is not available publicly. The level of review and oversight has not been publicly disclosed, nor is the decision-making process transparent. The public is not informed of the discussions or negotiations that result in actual filtering decisions.

Specificity in governmental filtering decisions is also difficult to implement. Legislation that determines what is impermissible speech is necessarily general; defining hate speech or obscenity defies easy criteria that can be codified into law. Nevertheless, if content on the Internet is to be banned, someone must translate general standards into specific blocking decisions. Such specificity in blocking, if applied by formal governmental process, is difficult to reconcile with effective Internet regulation. Turkey is attempting just such an approach, but is very limited in the scope of their blocking at present. Judicial review of individual websites and user-generated content on social media sites would be onerous on a large scale and nearly impossible on social media sites with existing technology.

Legally mandated and formalized Internet content restrictions are problematic in other ways as well. To be effective, mandatory blocking of specific websites or submissions to websites generally involves prior restraint on free speech. Although

most of the world does not share the same level of aversion to prior restraint as the United States, highly formal filtering procedures that require filtering of a substantial number of websites are less likely to withstand legal challenges in many countries. It is thus not surprising to see a significant reliance on informal and voluntary programs, and on the action of private companies based in foreign countries as the recipients of informal filtering requests and as the administrators of filtering. The most pragmatic solution is often a more informal and less exacting legal process.

The compromise in Germany has been to enact voluntary agreements with foreign companies, the details of which are not subject to public scrutiny. From China to Germany to Thailand, these determinations of illegal content also seem to fall into the realm of "I know it when I see it." This lends itself poorly to a formalized regulatory process specified by law.

The preference of certain governments to institutionalize informal public-private transnational filtering can also erode processes meant to ensure accountability. For example, although Thailand became one of the only countries in Asia to require court authorization when it passed a cyber crimes law in June 2007, in practice it appears to prefer informal filtering via country restrictions flags and enlisting Google to engage in geolocational filtering on its behalf.

One of the consequences of the Internet's architecture is that reasonable and appropriate content restriction policies may be effective only if implemented in ways that are not easily palatable for open societies. Although this tension existed before social media reached its current level of popularity and utility, its stupendous growth has brought these trade-offs and contradictions to the fore.

THE CHINA ALTERNATIVE

China represents an exception to the choices facing other countries and for the companies operating there. One consequence of the government's simultaneous priorities of growth and control has been the effective emergence of public-private localized filtering. China has promoted the development of Internet infrastructure and e-commerce while pursuing aggressive filtering, media clampdowns, and other rigorous restrictions on expression. A robust internal market for Internet services and content catering to the cultural and language specifications of 210 million Chinese Internet users has somewhat insulated users from the collateral social and economic costs of filtering.[49] The local Chinese-language search engine Baidu dominates the market, and YouTube's accessibility issues have paved the way for a rash of Chinese-language video sharing sites.[50]

Whereas international companies continue to grapple with the human rights impacts of doing business in certain jurisdictions, Chinese companies have little room to maneuver or negotiate around the government's stringent requirements for self-policing of news and other content. As a result, they are the most effective executors of a growing filtering mandate. China provides a model that promotes the growth of domestically managed, and regulated, social media sites. This is

undoubtedly an attractive notion for many other countries around the world.

INTERNATIONAL RESPONSES TO FILTERING: RENEWED FOCUS ON INTERMEDIARIES

The success of social media companies has brought with it both greater scrutiny and more responsibility. Just as governments lean upon the intermediaries to help with content regulation, those in favor of greater openness, enhanced privacy and high transparency have looked also to Western technology companies.

The companies that provide the transnational public spaces of the Internet have thus become the focal point of the debate over permissible speech on the Internet. They are subject to pressure from both sides of the debate—those espousing greater openness and those pushing for further restrictions. This will remain so unless and until governments are able to improve their ability to control online speech, particularly via social media sites that are already difficult to monitor. It is not clear which side will gain advantage in the next battle of the technology wars, providing another opportunity for debate between cyber-utopians and cyber-realists.

Governments and technology companies continue to negotiate ways to operate social media platforms across multiple jurisdictions without triggering further blocking of entire platforms and websites. A much smaller number of countries are investing in deploying technology that will allow selective blocking of content on social media sites.[51] The tacit principle underlying this government-driven approach is that each country will determine what constitutes acceptable speech for its citizens and has the discretion to restrict speech that falls outside of these norms. On a basic level, this is difficult to dispute. However, the waters are muddied by the perceived failure of many countries to live up to their international commitments to uphold human rights related to freedom of expression,[52] as well as the inherent difficulties in identifying impermissible speech.

A series of separate but related dialogues are occurring that may help to shape the future of this issue that do not directly involve the governments that have aggressively sought to censor the Internet. These approaches suggest hopes for a convergence in either the substantive or procedural standards in defining acceptable speech, rather than country-specific solutions to defining and enforcing permissible content. Within the United States and Europe, proposed legislative initiatives would seek to influence the actions of technology companies and perhaps their ability to do business in countries that limit privacy and free speech on the Internet.[53] Early versions of legislation in the United States sought to limit the latitude of action for technology companies working in repressive countries. Zittrain and Palfrey have called this process, which places legal restrictions on technology firms as a response to actions initiated by foreign governments, second-order regulation.[54] This approach is problematic in a number of ways. For this approach to be implemented, some institution or agency must be given authorization for determining where speech restrictions have been inappropriately applied. Delegating

governments the authority to regulate acts in other sovereign jurisdictions, even indirectly, is questionable.[55] Furthermore, the attempt to define the bounds of acceptable speech would be subject to the same potential pitfalls of excessive discretion and restriction. Laws that prohibit technology companies from participating in censorship may force them to disengage from a number of countries. Even requiring greater transparency, for example compelling Google, Yahoo!, and Microsoft to disclose the websites and content they filter, may have the same effect. However politically popular at the time, legally binding the hands of technology companies doing business in repressive regimes does not seem to have withstood intense scrutiny; this form of legislation has been set aside in the United States. Alternative legislative approaches have been proposed in the United States. One proposal would require thorough human rights impact assessments prior to entering markets in countries that restrict online speech.

Another dialogue is underway with technology companies, socially responsible investors, international human rights organizations, and academic institutions to craft a collective voluntary response to these challenges based on a code of conduct that would guide the actions of technology companies in international markets.[56] This collective approach has the potential to help all parties, including the technology companies and human rights groups, to better understand the risks and implications of conducting business in repressive regimes. If successful, it would also inform and shape the policy positions and responses of governments, as well as build public awareness. There have been a number of similar multi-stakeholder initiatives in the past designed to promote better corporate ethical behavior in international business.[57] One of the remarkable facets of this dialogue is the level of overlapping commitment between private sector and advocacy groups to increasing the flow of unfiltered information. While one side protects free expression as part of its revenue strategy, the other is engaged solely in order to promote human rights and social justice.

This voluntary approach might either replace or complement U.S. regulatory action. One promising line of attack would be to use the voluntary principals as the basis for future legislation, providing the authority and legal framework to ensure broader compliance with the principles.[58]

A limitation with these international initiatives that aim to reduce Internet filtering is that they focus almost entirely on the intermediaries and not on the source of these restrictions—foreign governments. Given this fundamental limitation, it is unclear how far the efforts of technology companies and non-governmental organizations, even when working collaboratively, can go to address these growing tensions.

Another alternative—intergovernmental action—has not gained any traction to date. Nevertheless, Google has attempted to raise the issue to this level, publicly requesting help from the U.S. government in invoking restrictions on free speech as a trade issue.[59] This strategy has resonated in Europe as well.[60] Although preliminary, this approach may relieve the growing pressure on technology companies coming from both sides, even if it does not provide a genuine solution to the ques-

tions being posed. In the meantime, the technology companies that provide the nodes for social media will continue to be the focus of attention.

The public-private transnational negotiations that lead to selective filtering are not without potential benefits. Despite the lack of transparency and accountability, this channel has provided limited checks on government authority as technology companies have not always acquiesced to the filtering demands of governments. Ultimately, the various actors involved in the filtering of social media face choices that mirror the precarious balancing of values and interests evident in the Google.cn decision.

Many believe filtering is categorically wrong and that selective filtering by Western technology companies represents an unacceptable compromise. However, advocates for free expression on the Internet are not likely to win a debate that hinges on the notion that sovereign states should not be able to regulate online speech. Moreover, while international intermediaries may be adopting limits on expression that many would find repugnant or overly restrictive, they are likely increasing overall access to information in the short term by selectively filtering content. This is almost certainly true when the alternative to selective filtering is the wholesale blocking of an entire website that acts as an important social media node.

The platforms for political and social openness are difficult if not impossible to distinguish from those driving knowledge accumulation and economic growth. While the collateral costs of blocking popular sites continue to grow, the political, social and cultural ramifications of allowing unfiltered access to the Internet also increase.

A bigger point of uncertainty is the long-term impact of these complex decisions on Internet freedom, an area where principle-based and pragmatic strategies are difficult to separate. Adopting an absolutist stance in discussions with governments may well contribute to greater long-term openness if access to international social media sites becomes a significant issue in countries' policies towards Internet filtering. It may also be that taking a principled stand on free expression is simply the right thing to do and will leave a positive and enduring example for countries engaged in these decisions. On the other hand, international technology companies that refuse to cooperate with governments may actually encourage states to hasten development of domestically owned and regulated alternative providers, nullifying their leverage and increasing competition. As domestic markets for social media and other online content grow, as with China, there may be

fewer opportunities to engage in public discourse over the normative standards governing the substance and process of Internet content regulation.

CONCLUSIONS

The profusion of political commentary, photographs, and video hosted on social media sites, such as social networking, photo sharing, and video sharing platforms, creates a policy conundrum for many governments around the world.

Governments must consider whether to open the gates to social media, block these services entirely, or attempt to enlist technology companies to selectively block content. Many have already blocked popular sites in their entirety, despite the obvious costs to millions of users. If this trend continues, the implications of these content restriction decisions, both in costs and benefits, will become more acute; the platforms for political and social openness are difficult if not impossible to distinguish from those driving knowledge accumulation and economic growth. While the collateral costs of blocking popular sites continue to grow, the political, social, and cultural ramifications of allowing unfiltered access to the Internet also increase. For countries that place high priority in transparency, public consultation, and open review of decisions that restrict freedom of speech, abandoning Internet filtering altogether might be the best alternative.

Regulatory responses have thus far been unable to keep apace with the speed of technological change, and an increasing number of governments are moving towards this public-private transnational form of filtering. At the same time, the search for international solutions that address the tensions in online content regulation, particularly involving innovative social media platforms, has been slowed by the complexity and high degree of uncertainty over the efficacy of policy interventions. It is still unclear how short-term actions to resist or comply with Internet censorship may impact the long-term objectives, such as persuading governments to embrace greater Internet openness. Moreover, international actions designed to promote free expression online in one country may reduce Internet freedom in another. Negotiated, informal, selective filtering agreements between governments and companies may alleviate some of these tensions and curtail the most extreme effects, but occupy a gray zone in which transparency and public accountability can be sacrificed. For those that espouse greater openness, the best responses are more likely to come from a flexible public-private partnership than from more rigid government mandates.

The economic and educational benefits of an unrestricted Internet represent one of the strongest arguments for Internet openness. Advocates have a chance to more convincingly demonstrate the innovative aspects and benefits associated with social media and Web 2.0 applications. The policies and technologies of regulation may soon catch up with the distributive power of social media.

---

1. Jonathan Zittrain and John Palfrey anticipate and describe this dynamic. See Internet Filtering: The Politics and Mechanisms of Control, in Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., *Access Denied: The Practice and Policy of Global Internet Filtering*,

(Cambridge: MIT Press) 2008.
2. John Aglionby, "Filipinos rally to oust the president," *The Guardian*, January 20, 2001, http://www.guardian.co.uk/world/2001/jan/20/johnaglionby1.
3. Joshua Goldstein, *The Role of Digital Networked Technologies in the Ukrainian Orange Revolution*, Berkman Center Research Publication No. 2007-14, December 1, 2007, http://cyber.law.harvard.edu/publications/2007/The_Role_of_Digital_Networked_Technologies_in_the_Ukranian_Orange_Revolution.
4. See Howard Rheingold, *Smart Mobs: The Next Social Revolution* (New York: Basic Books) 2002.
5. See John Fiske, *Television Culture: popular pleasures and politics* (Methuen & Co. Ltd. 1987).
6. Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (New Haven and London:Yale University Press) 2006.
7. John Perry Barlow, *A Declaration of the Independence of Cyberspace*, February 8, 1996, http://homes.eff.org/~barlow/Declaration-Final.html.
8. Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (New York: Oxford University Press) 2006.
9. See http://www.opennet.net.
10. For a thorough overview of filtering techniques, see Steven J. Murdoch and Ross Anderson, Tools and Technology of Internet Filtering, in Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., *Access Denied: The Practice and Policy of Global Internet Filtering*, (Cambridge: MIT Press) 2008.
11. Jonathan Zittrain, "Internet Points of Control," 44 *Boston College Law Review* 653 (2003). John G. Palfrey and Robert Rogoyski, "A Move to the Middle: The Enduring Threat of Harmful Speech to the End-to-End Principle," 21 *Washington University Journal of Law & Policy* 31 (2006).
12. The legal, technical, and economic issues can be nevertheless exceedingly complex. These issues are described in detail in Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., *Access Denied: The Practice and Policy of Global Internet Filtering*, (Cambridge: MIT Press) 2008.
13. Generally, under US law no goods, technology, or services may be exported, or sold to Iran unless licensed by Office of Foreign Assets Control. See http://www.treas.gov/offices/enforcement/ofac/programs/iran/iran.shtml.
14. *The Guardian*, "Landmark ruling against Yahoo! in Nazi auction case," November 20, 2000, http://www.guardian.co.uk/technology/2000/nov/20/internetnews.freespeech.
15. Carl S. Kaplan, "French Nazi Memorabilia Case Presents Jurisdiction Dilemma," *The New York Times*, August 11, 2000, http://partners.nytimes.com/library/tech/00/08/cyber/cyberlaw/11law.html.
16. For an analysis of the Yahoo! auction case, see Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (New York: Oxford University Press) 2006.
17. http://cyber.law.harvard.edu/filtering/google/
18. Hearing transcript, "The Internet in China: A Tool for Freedom or Suppression?" Joint hearing before the Subcommittee on Africa, Global Human Rights and International Operations and the Subcommittee on Asia and the Pacific of the Committee on International Relations, House of Representatives, 109th Congress, Second session, February 15, 2006, Serial No. 109–157, p. 96, http://www.foreignaffairs.house.gov/archives/109/26016.pdf.
19. http://googleblog.blogspot.com/2006/01/google-in-china.html.
20. See http://chillingeffects.org.
21. Wikipedia defines social media as: "an umbrella term that defines the various activities that integrate technology, social interaction, and the construction of words and pictures." We use this term primarily for convenience. For the purposes of this paper, the most relevant aspects of the categorization are the participatory and sharing nature of the media and the use of multiple formats, including video, audio and text. There are several competing terms that might apply equally well, include participatory media, citizen media, new media, citizen journalism, and so on. They all capture and highlight different aspects of the phenomenon imper-

fectly.

22. In January 2007, nearly 3.4 billion videos were viewed on YouTube in the US, a 34.3 percent share of all videos viewed. Comscore press release, "YouTube.com Accounted for 1 Out of Every 3 U.S. Online Videos Viewed in January," March 14, 2008, http://www.comscore.com/press/release.asp?press=2111.
23. OpenNet Initiative, China country profile, 2006, http://opennet.net/research/profiles/china.
24. http://www.ogleearth.com/BahrainandGoogleEarth.pdf. The images, annotated with descriptions of the luxurious compounds of the ruling families, were compiled into a document easily shared via email and posted on any number of Web sites.
25. OpenNet Initiative, Bahrain country profile, 2006 http://opennet.net/research/profiles/bahrain#footnote27.
26. Maria Camila Pérez, "Facebook brings protest to Colombia," *International Herald Tribune*, February 10, 2008, http://www.iht.com/articles/2008/02/08/business/protest11.php
27. Shasta Darlington, Videos hint at public discontent in Cuba, CNN.com, February 7, 2008, http://www.cnn.com/2008/WORLD/americas/02/07/cuba.videos/index.html.
28. http://www.youtube.com/user/waelabbas.
29. OpenNet Initiative, Pulling the Plug: A Technical Review of the Internet Shutdown in Burma, November 27, http://opennet.net/research/bulletins/013/.
30. In fact, it is unlikely that the video clips of the events were uploaded on the Internet in Burma given the relatively poor connectivity there and the large size of video files.
31. According to YouTube's Community Guidelines, "We encourage free speech and defend everyone's right to express unpopular points of view. But we don't permit hate speech (speech which attacks or demeans a group based on race or ethnic origin, religion, disability, gender, age, veteran status, and sexual orientation/gender identity." YouTube Community Guideines, http://www.youtube.com/t/community_guidelines, accessed April 14, 2008. See also Section E, Youtube Terms of Use (stating that "You further agree that you will not, in connection with User Submissions, submit material that is contrary to the YouTube Community Guidelines…or contrary to applicable local, national, and international laws and regulations), http://www.youtube.com/t/terms, accessed April 14, 2008.
32. Ambika Ahuja, "YouTube seeks to end ban in Thailand, Associated Press," April 7, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/04/07/AR2007040700362.html.
33. *The Sydney Morning Herald*, "YouTube removes clips mocking Thai king," May 12, 2007, http://www.smh.com.au/news/World/YouTube-removes-clips-mocking-Thai-king/2007/05/12/1178899145725.html.
34. *The Nation*, "Ban on YouTube lifted after deal: Website to block clips offensive to Thais or that break Thai law," August 31, 2007, http://nationmultimedia.com/2007/08/31/headlines/headlines_30047192.php.
35. Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (New York: Oxford University Press) 2006.
36. Lawrence Lessig, *Code 2.0* (New York: Basic Books) 2006.
37. http://youtomb.org.
38. YouTube offers different accounts for users, such as standard or director accounts. Neither of these types of accounts allow users to tag accounts for geolocational filtering.
39. For example, a number of National Basketball Association videos featuring player Yao Ming carry the China restriction flag, but Youtomb has yet to find evidence of politically sensitive content on Youtube restricted geolocationally for China.
40. Citizen Media Law Project Database, Julius Baer Bank and Trust v. Wikileaks, February 18, 2008, http://www.citmedialaw.org/threats/julius-baer-bank-and-trust-v-wikileaks.
41. Wikileaks claims to have received over 1.2 million documents, http://wikileaks.org/wiki/Wikileaks:About.
42. For an analysis of the Wikileaks case see David Ardia, "Making Sense of the Wikileaks Fiasco: Prior Restraints in the Internet Age," Citizen Media Law Project blog, February 19th, 2008, http://www.citmedialaw.org/blog/2008/making-sense-wikileaks-fiasco-prior-restraints-internet-age

43. Tom Regan, "Gossip sites push web 'anonymity' to fore," *Christian Science Monitor*, March 5, 2008, http://www.csmonitor.com/2008/0305/p15s01-stct.html.
44 Electronic Frontier Finland, "Finnish Internet Censorship," http://www.effi.org/blog/kai-2008-02-18.html.
45. European Commission, "E-government Factsheets: Turkey," November 2007, http://www.epractice.eu/document/3525. Reporters Without Borders press release, "Bill censoring online content that insults Atatürk is signed into law," May 24, 2007, http://www.rsf.org/article.php3?id_article=22273.
46. Times Online, "YouTube banned in Turkey after video insults," March 7, 2007, http://www.timesonline.co.uk/tol/news/world/europe/article1483840.ece.
47. Sami Ben Gharbia, Turkey: WordPress ban inspires firestorm of criticism, Global Voices Online, August 21, 2007, http://www.globalvoicesonline.org/2007/08/21/turkey-wordpress-com-ban-inspires-firestorm-of-criticism/. World Bulletin, Turkey bans Google Groups, April 10, 2008, http://www.worldbulletin.net/news_detail.php?id=20780.
48. A collection of blockpages can be seen at http://www.blockpage.com
49. China Internet Network Information Center, The 21st Statistical Survey Report on the Internet Development in China, January 17, 2008, http://www.cnnic.net.cn/html/Dir/2008/02/29/4999.htm.
50. Bruce Einhorn, "Why YouTube is MIA in China," *BusinessWeek*, December 6, 2007, http://www.businessweek.com/globalbiz/content/dec2007/gb2007126_906695.htm?chan=top+news_top+news+index_global+business. See also Ethan Zuckerman, "Cute cat theory: the China corollary," December 3, 2007, http://www.ethanzuckerman.com/blog/2007/12/03/cute-cat-theory-the-china-corollary/.
51. For example, an ISP in Pakistan is implementing technology that would permit the selective blocking of YouTube videos. Previous regulatory actions required the blocking of the entire site.
52. See Mary Rundle and Malcolm Birdling, "Filtering and the International System: A Question of Commitment" in Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., *Access Denied: The Practice and Policy of Global Internet Filtering*, (Cambridge: MIT Press) 2008.
53. Full text of the Global Online Freedom Act available at http://thomas.loc.gov/home/gpoxmlc110/h275_ih.xml. John Palfrey, "Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet," *Global Internet Technology Report*, p. 69, World Economic Forum, 2006-2007.
54. Jonathan Zittrain and John Palfrey, "Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet," in Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., *Access Denied: The Practice and Policy of Global Internet Filtering*, (Cambridge: MIT Press) 2008.
55. Rebecca Mackinnon, "Global Online Freedom Act is re-introduced," January 11, 2007, http://rconversation.blogs.com/rconversation/2007/01/global_online_f.html.
56. http://cyber.law.harvard.edu/research/principles.
57. See, for example, Simon Zadek, "The Logic of Collective Governance: Corporate Responsibility, Accountability and Public Contract," Corporate Social Responsibility Initiative, Working Paper No. 17, Cambridge, MA: John F. Kennedy School of Government, Harvard University, 2006.
58. Jonathan Zittrain and John Palfrey, "Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet," in Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., *Access Denied: The Practice and Policy of Global Internet Filtering*, (Cambridge: MIT Press) 2008.
59. Christopher Rugaber, "Google Fights Global Internet Censorship," *Washington Post*, June 25, 2007, accessed at http://www.washingtonpost.com/wp-dyn/content/article/2007/06/25/AR2007062500364_pf.html
60. Sami Ben Gharbia, "EU: Towards a European Global Online Freedom Act," Global Voices Advocacy, March 6, 2008, http://advocacy.globalvoicesonline.org/2008/03/06/eu-towards-a-european-global-online-freedom-act/.

innovations
TECHNOLOGY | GOVERNANCE | GLOBALIZATION

Support for this *Innovations* special issue
provided in part by
Realizing Rights: The Ethical Globalization Initiative

INNOVATIONS IS JOINTLY HOSTED BY

GEORGE MASON UNIVERSITY
School of Public Policy
Center for Science and Technology Policy

HARVARD UNIVERSITY
Kennedy School of Government
Belfer Center for Science and International Affairs

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
Legatum Center for Development and Entrepreneurship

with assistance from
The Lemelson Foundation
The Ash Institute for Democratic Governance and Innovation, Harvard University
The Center for Global Studies, George Mason University

GEORGE MASON UNIVERSITY | School of Public Policy

BELFER CENTER for Science and International Affairs
John F. Kennedy School of Government
Harvard University

mitpress.mit.edu/innovations | innovationsjournal.net
editors@innovationsjournal.net