5 Intermediary Censorship

Ethan Zuckerman

Introduction

When academics, journalists, or Internet users discuss ''Internet censorship,'' they are usually referring to the inability of users in a given country to access a specific piece of online content. For instance, when Internet policymakers from around the world came to Tunisia for the 2005 World Summit on the Information Society, they discovered that the Tunisian government was blocking access to several sites, including Yezzi.org, an online freedom of speech campaign.[1]

This model of Internet filtering, where Internet service providers (ISPs) implement directives issued by government authorities and block connections to selected Web addresses, has been extensively documented by the OpenNet Initiative using in-country testing. Identifying potential cases of filtering by ISPs is likely to be easier in the future with the advent of tools like Herdict (www.herdict.org), which invite end users to be involved with in-country testing on a continuing basis.

Given aggressive national filtering policies implemented in countries like Saudi Arabia, China, and Vietnam, state-sponsored ISP-level Web filtering has been an appropriate locus for academic study. However, ISPs are only one possible choke point in a global Internet. As the Internet increases in popularity around the world, we are beginning to see evidence of Internet filtering at other points in the network. Of particular interest are online service providers (OSPs) that host social networking services, blogs, and Web sites. Because so many Internet users are dependent on OSPs to publish content, censorship by these entities has the potential to be a powerful control on online speech.

In this chapter, I look at recent developments in intermediary censorship in China, where unclear government directives mandate censorship by blogging hosts, but provide little guidance for what content must be filtered. Confusion over U.S. trade restrictions is having a chilling effect on speech in the United States, where some OSPs are removing the accounts of users from sanctioned nations, including sensitive human rights Web sites. I examine the incentives and costs OSPs face surrounding removal of

online content and argue that protection of online speech rights by these intermediaries will require an affirmation of their role as free speech providers and clarification of applicable laws and regulations.

Points of Control

While filtering by ISPs was well documented as early as 2002, and commercial tools to filter Internet access in schools, libraries, and businesses have been available since the late 1990s, filtering at other points in the network is a more recent phenomenon. Skype's Chinese-language client, built in cooperation with TOM Online, demonstrated that Internet filtering could be implemented at the client software level. In April 2006, Skype admitted that the co-branded Chinese version of the Skype text chat product filtered users' messages based on a list of banned keywords.[2] In 2008, Internet researcher Nart Villeneuve discovered that the TOM Skype software was not merely blocking keywords, but surveilling users, storing conversations where specific keywords had been mentioned.[3]

Examples like this indicate that scholars of Internet filtering and censorship need to develop methods to monitor and study filtering at other points in the network: an end user's operating system, application software and hardware; intermediate nodes in networks, beyond ISPs and boundary routers; Web hosting providers; and providers of social media services.

Companies that provide Web hosting services or social media platforms are becoming increasingly important as possible choke points as Web users publish content on Web servers they do not control. In the early days of the World Wide Web, most Web sites were managed by organizations that controlled the content posted on the sites, the server software that delivered Web pages, and the server hardware that ran the code. While some Web sites are still vertically integrated and managed, the vast majority of Web site developers rent server space from Web hosting companies or use free Web hosting services like Tripod.com or Wordpress.com.

These OSPs provide services to millions of users, most of whom would lack the means and technical skill to maintain their own Web servers. Sites that allow publishing in the context of more complex community interactions, like Facebook or LiveJournal, would be extremely difficult for even a sophisticated user to reproduce. The unique dynamics of those communities require thousands or millions of users to share a single platform managed by a community host. While the ease of use of these platforms has been a great boon for online free speech, it has put a great deal of power in the hands of companies that provide Web site or community hosting services.

Under pressure from local legal authorities, these companies can reveal sensitive information about users. Yahoo!'s Hong Kong office complied with Chinese government requests for the identity of a user who forwarded a memo documenting government

pressure on Chinese journalists to an overseas Web site. Armed with information from Yahoo!, Chinese authorities arrested journalist Shi Tao and eventually sentenced him to ten years on charges of leaking state secrets.[4] These companies can also act as censors, removing material that governments deem unacceptable in local jurisdictions. More unsettlingly, they may also remove material based on misunderstandings of local laws or based on calculations of fiscal and legal risk.

Host-Based Censorship in China

Studies of ISP-based Internet filtering have characterized Chinese Internet filtering that was pervasive as early as 2002.[5] Bloggers and journalists refer to China's complex set of filtering practices as the Great Firewall. It should not be a surprise, then, that China has pioneered censorship at the Web and community hosting level, as well as filtering content by means of ISPs.

In March 2004, Chinese authorities closed down three blog hosts—blogcn.com, blogbus.com, and blogdriver.com—because of concerns that sensitive content was being published on these sites.[6] After these sites reopened, the OpenNet Initiative found evidence that Chinese-based blogging providers were using lists of sensitive keywords to prevent controversial content from being posted to their Web servers.[7] In June 2005, Rebecca MacKinnon demonstrated that Microsoft was using similar techniques to block content on their Chinese-language version of MSN Spaces—her attempts to start a blog titled ''I love freedom of speech, human rights and democracy'' (in Chinese) yielded an error message that she translates as ''You must enter a title for your space. The title must not contain prohibited language, such as profanity. Please type a different title.''[8]

A report by Reporters Without Borders (RSF) and China Human Rights Defenders, released in October 2007, was compiled with the help of an anonymous technician (Mr. Tao) working for a Chinese Internet company, presumably a company involved with hosting user-generated content. The report, ''A Journey to the Heart of Internet Censorship,''[9] details training efforts to ensure that employees of content hosting companies censor sensitive content, and describes a weekly meeting at the Internet Information Administrative Bureau of the employees of Beijing's 19 leading Web sites. The meetings outline sensitive topics likely to be discussed in the coming week and provide instructions on which topics are to be censored.

While RSF's report details efforts aimed at coordinating content censorship in China, subsequent research by MacKinnon reveals that such censorship is extremely unpredictable and subjective. In ''China's Censorship 2.0: How Companies Censor Bloggers,''[10] MacKinnon and students tested censorship systems on 15 Chinese blogging providers, using a variety of potentially sensitive texts taken from Chinese-language blogs and news sites. Her team posted the text to author accounts on the 15 platforms,

and checked to see whether (1) they were able to successfully post the material, (2) whether it remained posted 24–48 hours later, and (3) whether they could view the posted content from a Chinese ISP without using circumvention software.

Results varied widely. One of the blogging service providers tested blocked 60 of 108 tested texts. Another blocked only one. MacKinnon was unable to find a single text blocked by all blogging providers, though she concluded that current news topics, which she terms ''sudden incidents'' were far more likely to be blocked than other sensitive topics. She observes, ''The wide variation in levels of censorship confirms that censorship of Chinese user-generated content is highly decentralized, and that implementation is left to the Web companies themselves.''

While many countries block access to social media sites,[11] the vast majority of these blocked sites are managed and hosted in the United States. China's unusual approach of filtering access to sensitive sites and requiring social media providers to censor their users reflects the large number of social media companies based in China, catering to a huge domestic market. The history of filtering and censorship in China may have led to an especially effective model. Since many popular online publishing platforms are filtered by Chinese ISPs, Chinese netizens have gravitated to hosts located in China. Because these sites provide interfaces in Chinese, they are easier to use than U.S.-based sites. And while these sites engage in censorship to avoid government sanctions, most users will not notice the censorship until they try to post about sensitive topics.

It is somewhat surprising that we have not seen other countries that filter the Internet by means of ISPs implement China's model of platform-based censorship. However, Chinese companies have taken leadership in the social media world, while leading platforms for social media in many other countries that filter the Internet are located outside national control, generally within the United States.

OSP-Based Censorship in the United States

There is no evidence that the U.S. government is demanding censorship of OSPs in the same way that the Chinese government has attempted to control social media. However, unclear U.S. laws may have led to situations in which U.S.-based OSPs have removed user accounts, effectively silencing those users, based on legal misinterpretations.

Brenda Burrell is used to worrying about censorship. As one of the cofounders of Kubatana, a civil-society organization based in Harare, Zimbabwe, she works with human rights organizations whose members are routinely harassed and imprisoned for speaking in public or online. In a blog post, she notes that she is used to fielding questions about what might happen if the Mugabe regime shut down her Internet operations. But on February 6, 2009, she was surprised to hear from BlueHost, an American Web-hosting company, that Kubatana's Web site, along with the Web sites

of Women of Zimbabwe Arise and Island Hospice and Bereavement Service, would be disabled so that BlueHost would remain in compliance with U.S. Treasury Department restrictions.[12]

BlueHost, which had hosted Kubatana's Web site, told Burrell that her site was in contravention of section 13 of their terms of service, which read in part:

> Sanctioned Countries presently include, among others, Balkans, Belarus, Burma, Cote d'Ivoire (Ivory Coast), Cuba, Democratic Republic of the Congo, Iran, Iraq, former Liberian Regime of Charles Taylor, North Korea, Sudan, Syria, and Zimbabwe. 'Sanctioned Countries' shall be deemed automatically to be added to or otherwise modified from time to time consistent with the determination(s) of the government of the United States, and shall include all other countries with respect to which commercial activities are prohibited, embargoed, sanctioned, banned and/or otherwise excluded by determination(s) of the government of the United States from time to time.
>
> 1. Each Sanctioned Country, all governmental, commercial, or other entities located therein, and all individuals located in any Sanctioned Country are hereby prohibited from registering or signing up with, subscribing to, or using any service of BlueHost.Com.[13]

These are not the terms of service Burrell agreed to when opening an account with BlueHost. Archived copies of the BlueHost terms of service, retrieved via Archive.org, do not contain section 13—the section was evidently added sometime after February 8, 2008 (the last date BlueHost's terms of service is available via Archive.org).[14] Burrell was unaware of the change in terms of service until BlueHost alerted her that she would need to remove her Web site or face its removal.

Burrell challenged BlueHost's decision, not by arguing that she was in compliance with their terms of service—she clearly was not—but by arguing that these terms of service misrepresented the U.S. Treasury Department's sanctions. The sanctions Zimbabwe faces are targeted to the Mugabe regime, not toward all Zimbabweans. The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) is quite specific about who the sanctions target:

> Executive Order 13391 prohibits U.S. persons, wherever located, or anyone in the United States from engaging in any transactions with any person, entity or organization found to: 1.) be undermining democratic institutions and processes in Zimbabwe; 2.) have materially assisted, sponsored, or provided financial, material, or technological support to these entities; 3.) be or have been an immediate family member of a sanctions target; or 4.) be owned, controlled or acting on behalf of a sanctions target. Persons, entities and organizations referenced in Annex A of the Executive Order are all incorporated into OFAC's list of Specially Designated Nationals (SDNs).[15]

It would be difficult for a company like BlueHost to evaluate whether Burrell and Kubatana were engaged in undermining democratic institutions. Fortunately, OFAC maintains a list of Specially Designated Nationals that U.S. companies are banned from doing business with—checking against this list is significantly simpler.

Burrell forwarded the relevant OFAC sanctions documents to BlueHost's abuse department, sought assistance from the U.S. Embassy in Zimbabwe, and mounted an

online campaign to pressure BlueHost to change its policies.[16] Neither the explanatory e-mails nor public campaign swayed BlueHost or their CEO Matt Heaton. Burrell reports that Heaton communicated with her directly on the matter of the campaign, telling her that her supporters were ''spamming'' him and that he was unwilling to help her resolve the situation given this external pressure.[17]

Pressure from the Treasury Department, however, was ultimately successful. Burrell received an e-mail from BlueHost on February 18 stating:

> Per request from the Treasury Dept, we have reactivated your account with Bluehost. With the release from the Treasury Department received today from Rachel Nagle of the Treasury Department via telephone and email confirming on February, 18, 2009 that you do not appear on OFAC's list of Specially Designated Nationals and Blocked Persons we will continue hosting your website.
>
> We apologize for any inconvenience this may have caused you.

Burrell and Kubatana decided that the ''inconvenience'' was significant enough that they moved their Web sites to a hosting company based in New Zealand and exempt from U.S. Treasury Department sanctions—the managing director of that company was alerted to Kubatana's status as a Zimbabwean nonprofit and affirmed his willingness to host their Web sites.

Zimbabwean human rights organizations were not the only ones affected by BlueHost's interpretation of U.S. Treasury regulations. Yaraslau Kryvoi, a Belarusian activist based in Washington, DC, saw his blog, promoting the Belarusian American Association, taken down by BlueHost.[18] 1 Fathi, a prominent Persian blogger, reported that his blog, as well as several other Persian blogs, were being removed by BlueHost as they contravened Section 13 of the company's terms of service.[19]

Evgeny Morozov, reporting on the situation in *Newsweek*, suggests that BlueHost's decision was based on expediency: ''Although BlueHost is one of the world's biggest hosting companies, it probably does not have the time or resources to match the OFAC list with its own customer ranks. Banning everyone from Belarus takes much less time and effort.'' He notes that BlueHost's terms of service are surprisingly sloppy—there's no nation called ''the Balkans,'' and Morozov wonders whether BlueHost plans on removing Romanian and Slovenian sites as well.[20] It is worth noting that, despite Burrell's successful protest and Morozov's article, BlueHost's terms of service still include a blanket block on usage from 11 nations, one region, and one long-deposed regime.

The removal of Iranian, Belarusian, and Zimbabwean content is deeply ironic, given that the sites that were removed were critical of the governments being sanctioned by the United States. The actions taken by BlueHost, either at the encouragement of the Treasury Department or because of their misinterpretation of Treasury regulations, had an effect opposite to what was intended by those sanctions—by silencing criticism, the removal of these sites benefits the sanctioned governments.

An Emerging Trend?

It is possible that BlueHost may be on the leading edge of a new trend. Social networking site LinkedIn.com began blocking Syrian users from connecting to their site in April 2009. Anas Marrawi reported that LinkedIn began blocking Syrian users based on their IP in late March, but that Syrian users continued to use the site through filtering-circumvention software. On April 19, Marrawi reported that the site delivered a message to any users who had listed their home country as Syria when they logged on: ''Access to this account has been suspended. Please contact Customer Service to resolve this problem.'' He contacted customer service and was told that LinkedIn could no longer provide services to Syrian users.[21]

Like Kubatana targeting BlueHost, Syrian LinkedIn users and their supporters began an online campaign to convince LinkedIn to reevaluate their policies. Jillian York,[22] a U.S.-based blogger with strong ties to the Syrian online community, helped coordinate the effort, writing about the block on the Huffington Post[23] and promoting the cause on Twitter. Through Twitter, she got in touch with LinkedIn's senior director of corporate communications, who quickly issued a mea culpa and promised a swift reversal of the decision.[24] Shortly after, LinkedIn issued the following statement: ''Some changes made to our site recently resulted in Syrian users being unable to access LinkedIn. In looking into this matter, it has come to our attention that human error led to over compliance with respect to export controls. This issue is being addressed tonight and service to our Syrian users should be restored shortly.''[25]

It is unclear what has motivated U.S. Web hosting and social media companies to ensure they are in compliance with Treasury restrictions and export controls. Like BlueHost, LinkedIn has recently changed their terms of service. The current terms of service references export controls in its opening section: ''Your use of LinkedIn services, including its software, is subject to export and reexport control laws and regulations, including the the Export Administration Regulations ('EAR') maintained by the United States Department of Commerce and sanctions programs maintained by the Treasury Department's Office of Foreign Assets Control.''[26] An archived version of their terms of service,[27] from January 3, 2008, makes no reference to export controls or sanctioned countries. Users of hosting and social media tools who live in nations subject to U.S. export controls or sanctions face an extremely confusing situation. LinkedIn, MySpace, and Blogger make reference to U.S. export laws, while YouTube, Facebook, Wikipedia, Rapidshare, and Wordpress do not.[28]

Web hosting companies are similarly divided—of the 22 top hosting sites, as tracked by Webhosting.info,[29] BlueHost, sister company Hostmonster, and hosting company One and One require users to certify that they are not from a list of specified countries. Network Solutions and BCentral offer a general caution that users must comply with U.S. export laws, and the other hosts do not mention export controls or sanctions in

their terms of service. (Based on an examination of current terms of service of the 22 top sites as listed by Webhosting.info. One of the top sites does not offer a formal terms of service—it controls hundreds of thousands of domains itself, but has no customer relationships. Two sites serving China did not have terms of service available on their Web sites. Evaluation covers the remaining 19 sites.)

In contrast to BlueHost's decision to deny service to over 300 million potential customers, sanctioned or not, other companies are taking a de minimis approach to compliance with U.S. government restrictions. Andrew McLaughlin, senior policy counsel for Google, notes, ''We do the minimum to comply with the export restrictions and sanctions regimes. Primarily, this means (1) we don't allow downloads of software (Google Earth, e.g.,) containing cryptography from IPs believed to be in restricted countries (Cuba, Iran, North Korea, Syria, Sudan)—this includes the Google download server and code.google.com; and (2) we don't engage in any sort of money transactions into or out of restricted countries. We do not, though, block access to publicly available sites where there are no downloads.''[30] Perhaps in reaction to the criticism the company took for filtering search results in the Chinese market, Google has demonstrated a willingness to challenge government-mandated filtering measures. When South Korea passed a law requiring online postings to be accompanied by the author's real name and ID card number, Google's YouTube division disabled commenting and video uploads from South Korea, but allows Korean users to state that they are posting from another country and post anonymously.[31]

The Economics of Intermediary Censorship

Google may have decided to disable comments in South Korea to make a statement about how requiring identification systems limits online speech. Or they may have been making a smart business decision—it would have required a major engineering effort for Google to build an identity authentication system for YouTube in Korea. The decisions BlueHost, LinkedIn, and others have made make more sense in a context of business risk and reward, rather than in a free speech and human rights context.

BlueHost advertises entry-level Web hosting for an annual cost of USD 83.40. Web hosting is a highly competitive business, and profit margins tend to be quite tight. With professional legal counsel experienced in U.S. export and sanctions law charging hundreds of dollars an hour for advice, it is an easy decision for BlueHost to sacrifice a handful of customer relationships in exchange for avoiding legal review. It is possible that LinkedIn made a similar evaluation and reversed course when public pressure indicated that LinkedIn's cost in terms of public relations damage might be substantial for removing Syrian users.

Wendy Seltzer identifies the problem of ''unbalanced incentives'' as a major concern in the United States' administration of the Digital Millennium Copyright Act (DMCA).

Section 512(c) of the DMCA provides ''safe harbor'' from liability due to copyright infringement if online service providers follow a prescribed procedure to remove copyrighted content when alerted by the copyright's owner.[32] On receiving a properly completed notice, an OSP should promptly remove the content in question and alert the individual who posted it, giving her an opportunity to respond with a counternotice to the party claiming infringement—on receipt of this counternotice, the OSP should restore the material to the Internet within 14 business days.

Seltzer argues that OSPs have a great incentive to take down potentially infringing material (the threat of litigation from movie studios or record companies), but significantly less incentive to protect the First Amendment rights of users. Providers do not generally alert their users that they might have a fair use argument to defend their use of a piece of content or direct users to sites like Chilling Effects (www.chillingeffects.org), a clearinghouse of information on takedown notices developed by Seltzer and others. The incentives for removing content are large, and they are small—and perhaps negative—for OSPs to encourage their users to fight takedown notices. If an OSP develops a reputation for aggressively defending user rights, it is likely to attract more users who generate infringement claims. Each one of these claims requires time and legal resources from an OSP to respond to—as a result, OSPs have an incentive to rapidly remove potentially infringing users and, perhaps, to discourage them from returning.

Sjoera Nas and the Dutch nonprofit Bits of Freedom wondered whether Netherlands ISPs would defend user rights against complaints of copyright infringement, so they mounted an experiment. In 2004, they opened accounts with ten Dutch OSPs and posted the same public domain text written by Eduard Douwes Dekker, better known by the pen name Multatuli. Then, they sent complaints in the name of a fictitious Mr. Johan Droogleever, legal advisor to the E. D. Dekker Society, which claimed to hold copyright to the works and demanded their removal. Seven of ten OSPs complied swiftly, without challenging the claim or demanding further information, despite the fact that the e-mail came from a Hotmail address. However, ISPs generally alerted the fictitious customer to the takedown request. Nas concludes, ''It only takes a Hotmail account to bring a website down, and freedom of speech stands no chance in front of the cowboy-style private ISP justice.''[33]

Whether Seltzer or Nas is correct in being concerned that copyright infringement complaints favor IP owners rights over user rights, the mechanisms for removing content suggest key weaknesses that censors could exploit. During the 2008 presidential election, both the Obama and McCain camps found that campaign videos were frequently removed from YouTube. The videos in question generally featured small excerpts from broadcast television newscasts, and takedown notices were issued by those broadcasters. The campaigns challenged the takedowns, arguing that their use of excerpts represented fair use.[34] Given the rapid-fire nature of political campaigns, the 14 business days it can take to restore a video to YouTube may effectively

constitute censorship. It seems likely that we will see political rivals attempt to disable each other's online speech using spurious copyright claims, even though these claims run the risk of exposing a complainant to penalties for acting in bad faith.

We are already beginning to see attacks on online speech that attempt to trigger an ''immune system response'' from hosting companies. Irrawaddy, a leading Web site for Burmese dissidents, suffered a series of distributed denial of service (DDoS) attacks in September 2008. Other pro-dissident sites, including the Oslo-based Democratic Voice of Burma and the New Era Journal, based in Bangkok, were rendered inaccessible by DDoS attacks, prompting speculation that the attacks were the work of hackers hired by the Burmese government.[35] As Irrawaddy struggled to fend off the DDoS attacks, its hosting provider became increasingly agitated, since the DDoS attack affected their other customers. For a period of time, the attack was so severe that Thailand's primary Internet connection was overloaded with DDoS traffic. The attack had the immediate effect of making the site unreachable, as well as the longer-term effect of forcing Irrawaddy to find a new ISP.[36]

As with copyright takedown notices, OSPs have a strong incentive to remove ''troublesome'' users—DDoS attacks can require hours of expensive system administration time to fend off. For hosting accounts that generate little revenue, the cost of fending off even a small DDoS is likely to exceed profit margins, and OSPs have an incentive to remove customers who have come under attack. Providers that develop a reputation for protecting their users from DDoS attacks are likely to attract customers who come under DDoS attacks, increasing their costs. As such, some OSPs are comfortable removing customers because they have come under attack. A libel lawsuit between Colocation America and Archie Garga-Richardson, whose Web site came under DDoS attack while hosted by Colocation America, makes it clear that OSPs are sometimes willing to remove customers generating thousands of dollars of revenue.[37]

Implications for Researchers

While the underlying threats to speech are deeply different between the case of Chinese blogging hosts studied by MacKinnon and U.S.-based OSPs outlined here, a common theme emerges: threats to online speech come not just from government action, but from the needs of OSPs to interpret and follow government regulations and to turn an operating profit. If this trend persists and grows, it has implications for scholars and activists focused on this issue.

Scholars need to develop tools and methods to study corporate filtering of Internet content. These methods might incorporate the techniques pioneered by MacKinnon in testing Chinese Web sites for automated censorship, perhaps with development of more robust tools to help automate testing. They could also include a site like Chilling Effects focused on collecting reports of corporate censorship of content, or an expan-

sion of the work of the Citizen Media Law Project to thoroughly document filtering and censorship by online service providers beyond the United States. Global Voices Advocacy, which now maps the accessibility of social media Web sites in different countries, may need to start mapping Web sites that ban users from certain countries.

To the extent that confusion over U.S. Treasury and export restrictions is leading toward the removal of Web sites and the understandable uncertainty of users in sanctioned countries, it may be worth pursuing clarifications from the U.S. government. Clinical students at the Berkman Center at Harvard are pursuing a formal request to the U.S. Treasury's Office of Foreign Asset Control to clarify the restrictions that social media and Web hosting companies face in providing services to users in sanctioned countries. If the Berkman Center receives useful clarifications, it will need to develop a strategy to communicate these guidelines to the affected companies.

Intermediary censorship by U.S. companies appears to be experiencing a steep and sudden rise. In May 2009, Vineetha Menon reported that Microsoft had turned off its Windows Live Messenger service in Iran, Syria, Sudan, Cuba, and North Korea, citing OFAC sanctions.[38] It is likely that Microsoft, BlueHost, and LinkedIn are not acting entirely independently—they may all be coming under pressure from the U.S. Treasury Department or another government authority. It would be useful for journalists or researchers to determine whether there is an organized campaign to remove users from these five sanctioned countries from U.S.-based tools. Given the use of these tools by human rights activists and ordinary citizens, a policy of removing all users in sanctioned nations from these tools merits careful public debate. It is possible that the most interested opponent of U.S. Treasury policy might be the U.S. State Department, anxious to hear opposition voices in repressive nations.

Imbalanced Incentives and Free Speech

So long as it continues to be possible for for-profit OSPs to terminate difficult clients for arbitrary reasons, it is likely that we will see providers ''optimizing'' their client base, providing services to customers who do not attract DDoS attacks or copyright or trade complaints. In a recent *New York Times* article, Brad Stone and Miguel Helft introduce the troubling idea that social media sites may start restricting memberships for users in developing nations because they are finding it difficult to target ads to these users.[39]

If these trends increase, organizations dedicated to free and open speech, especially in developing nations, may find themselves needing to create OSPs specifically oriented toward the needs of users who are less fiscally appealing to social media and Web hosting companies. We can imagine supporters of human rights creating OSPs explicitly to provide services for human rights organizations.

This is probably a poor idea. The cost structures of these organizations will be significantly higher than for traditional hosting providers, as they are likely to attract users

who come under attack by DDoS or who introduce complex legal questions. Furthermore, when human rights activists congregate on a small subset of servers, traditional ISP-level filtering becomes a more effective tool for censoring sensitive speech. If all sites critical of Burmese government policy are located on a single group of servers, that server is certain to be blocked at a national level, and is likely to come under sustained DDoS attack. By utilizing OSPs used by nonactivists, activists raise the social cost of traditional censorship—a country that chooses to block the Blogger.com domain to prevent access to a subset of blogs removes access from millions of uncontroversial Web sites, alienating citizens. Individuals who were not interested in the censored content become aware of the censorship when they can no longer access other Blogger.com sites.

Rather than creating a subset of Web sites that protect speech, it would be vastly better to see OSPs affirm their roles as providers of free speech tools to users throughout the world. As discussed earlier, this is a difficult decision for an organization, particularly a for-profit company, to make in isolation. At the moment, companies seem to be choosing a legally cautious path, disabling access for users in sanctioned countries before experiencing pressure from activists.

The experience of the successful protest against LinkedIn's block of Syrian users suggests that one powerful tool activists have is public protest. While companies may make a calculated financial decision to discontinue services to certain users, public pressure can add another factor into the equation—the potential lost business from bad publicity. While the LinkedIn protest shows the power of this strategy, BlueHost's decision not to reconsider their terms of service shows that the influence of public pressure may be limited.

Given the importance of OSPs as a space for open, public speech, it is necessary to consider their responsibilities as common carriers. For OSPs to limit their liabilities as common carriers, they should be required to provide services to anyone legally using these services, even if their usage is likely to attract DDoS attacks. To do otherwise is to allow attackers a ''heckler's veto,'' an ability to silence speech by creating a damaging and expensive response to that speech. If OSPs are required to provide services to any law-abiding users, an appropriate response to this form of intermediary censorship is legal action to address discrimination, not public protest. An affirmation of OSPs' role as common carriers would not resolve the situation Iranian and Syrian users are facing, but it might invite legal action that would force clarification of U.S. Treasury sanctions.

Conclusion

In countries like China, where online speech is carefully monitored and controlled, we are likely to see intermediary censorship emerge as an increasingly important compo-

nent of a censorship apparatus. Filtering at the OSP level blocks content from reaching both local and international audiences, allowing more thorough control of online content. The phenomenon is most developed in China, in part because existing Internet filtering strategies drive local users to publish on locally hosted sites, and in part because linguistic constraints drive Chinese-speaking users to a particular set of tools. If filtering and language constraints drive users in the Middle East toward locally hosted tools, we might expect to see similar systems of OSP-based filtering emerge.

As users around the world look to online services hosted in less controlled countries to find unfiltered venues to publish their content, other forms of content filtering are emerging. Online service providers have compelling financial incentives not to host content likely to provoke DDoS attacks or raise complex legal issues. While clarification of relevant regulations may help reduce uncertainty about what content can and cannot be hosted, there is a danger that OSPs will stop providing services to some users. This tendency needs to be counterbalanced by the sorts of public protest that called attention to BlueHost's and LinkedIn's actions, but user's rights will only be guaranteed by an affirmation of common carrier status that explicitly protects rights to publish on these platforms.

Notes

1. Rebecca MacKinnon, ''Tunisian Online Protest Blocked,'' Global Voices, October 4, 2005, http://globalvoicesonline.org/2005/10/04/tunisian-online-protest-blocked/.

2. Ben Charny, ''Chinese Partner Censors Skype Text Messages,'' PCmag.com, April 20, 2006, http://www.pcmag.com/article2/0,2817,1951637,00.asp.

3. Nart Villeneuve, ''Breaching Trust: An Analysis of Surveillance and Security Practices on China's TOM-Skype Platform'' (Information Warfare Monitor/ONI Asia, October 1, 2008), http://www.nartv.org/mirror/breachingtrust.pdf.

4. Reporters Without Borders, ''Information Supplied by Yahoo! Helped Journalist Shi Tao Get 10 Years in Prison,'' September 6, 2005, http://www.rsf.org/article.php3?id_article=14884.

5. Jonathan Zittrain and Benjamin Edleman, ''Empirical Analysis of Internet Filtering in China'' (Berkman Center for Internet and Society, Harvard Law School, March 2003), http://cyber.law.harvard.edu/filtering/china/.

6. Mat Honan, ''Little Red Blogs,'' Salon, June 4, 2004, http://dir.salon.com/story/tech/feature/2004/06/04/china_blogs/index.html.

7. OpenNet Initiative, ''OpenNet Initiative: Bulletin 008, Filtering by Domestic Blog Providers in China,'' January 20, 2005, http://opennet.net/bulletins/008/.

8. Rebecca MacKinnon, ''Screenshots of Censorship,'' RConversation Blog, June 17, 2005, http://rconversation.blogs.com/rconversation/2005/06/screenshots_of_.html.

9. Reporters Without Borders, ''A 'Journey to the Heart of Internet censorship' on Eve of Party Congress,'' October 10, 2007, http://www.rsf.org/article.php3?id_article=23924.

10. Rebecca MacKinnon, ''China's Censorship 2.0: How Companies Censor Blogs,'' *First Monday* 14, no. 2 (2009), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2378/2089.

11. See Global Voices Advocacy for a map of social media censorship. Global Voices Advocacy, ''Access Denied Map,'' October 29, 2008, http://advocacy.globalvoicesonline.org/projects/maps/.

12. Bev Clark, ''Curve Balls and Blue Beards,'' Kubanta.net, February 17, 2009, http://www.kubatanablogs.net/kubatana/?p=1261.

13. BlueHost, ''Bluehost.com Terms of Service,'' 2009, http://www.bluehost.com/cgi/info/terms.html.

14. BlueHost, ''Bluehost.com Terms of Service,'' archive.org, February 8, 2008, http://web.archive.org/web/20080201055355/www.bluehost.com/terms_of_service.html.

15. U.S. Department of the Treasury, Office of Foreign Assets Control, ''Zimbabwe: What You Need to Know about U.S. Economic Sanctions—An Overview of O.F.A.C. Regulations Involving Sanctions against Zimbabwe,'' November 13, 2005, http://www.treas.gov/offices/enforcement/ofac/programs/ascii/zimb.txt.

16. The author was involved in this online campaign and advised Burrell on her dealings with BlueHost.

17. Bev Clark, ''Curve Balls and Blue Beards,'' Kubanta.net, February 17, 2009, http://www.kubatanablogs.net/kubatana/?p=1261.

18. Evgeny Morozov, ''Do-It-Yourself Censorship,'' *Newsweek*, March 7, 2009. http://www.newsweek.com/id/188184.

19. Kanmangir, ''Persian Blogs on Bluehost Will Be Going Down,'' February 23, 2009, http://kamangir.net/2009/02/23/persion-blogs-on-bluehost-will-be-going-down/.

20. Evgeny Morozov, ''Do-It-Yourself Censorship,'' *Newsweek*, March 7, 2009. http://www.newsweek.com/id/188184.

21. ArabCrunch, ''LinkedIn Kicks Off Syrian Users!,'' April 17, 2009, http://arabcrunch.com/2009/04/breaking-linkedin-kicks-off-syrian-users.html; Morozov, ''Do-It-Yourself Censorship.''

22. York works for the Berkman Center for Internet and Society at Harvard University, focused on the OpenNet Initiative.

23. Jillian York, ''LinkedIn Alienates Syrian Users: Why Now?'' Huffington Post, April 20, 2009, http://www.huffingtonpost.com/jillian-york/linkedin-alienates-syrian_b_188629.html.

24. Mary Joyce, ''Why LinkedOut Syrians Are LinkedIn Again,'' Digiactive, April 21, 2009, http://www.digiactive.org/2009/04/21/why-linkedout-syrians-are-linkedin-again/.

25. Jillian York, ''LinkedIn Alienates Syrian Users: Why Now?'' Huffington Post, April 20, 2009, http://www.huffingtonpost.com/jillian-york/linkedin-alienates-syrian_b_188629.html.

26. LinkedIn, ''User Agreement,'' January 22, 2009, http://www.linkedin.com/static?key=user_agreement.

27. LinkedIn, ''User Agreement,'' archive.org, January 3, 2008, http://web.archive.org/web/20080103101839/http://www.linkedin.com/static?key=user_agreement.

28. Current terms of service were examined for the top social media sites, as listed by Alexa.com.

29. Webhosting.info, ''Top Web Hosts Worldwide,'' 2009, http://www.webhosting.info/webhosts/tophosts/global/.

30. Andrew McLaughlin, personal communication, April 2008.

31. Martyn Williams, ''Google Disables Uploads, Comments on YouTube Korea,'' PCWorld.com, April 13, 2009, http://www.pcworld.com/article/162989/google_disables_uploads_comments_on_youtube_korea.html.

32. Wendy Seltzer, ''''Intermediaries, Incentive Misalignments, and the Shape of Online Speech?'' (unpublished manuscript, Berkman Center for Internet and Society, Harvard Law School, 2009).

33. Sjorea Nas, ''The Multatuli Project: ISP Notice and Takedown,'' October 1, 2004, http://74.125.45.132/search?q=cache:lKhZFWp5TkcJ:www.bof.nl/docs/researchpaperSANE.pdf.

34. Fred von Lohmann, ''McCain Campaign Feels DMCA Sting,'' Electronic Frontier Foundation, October 14, 2008, http://www.eff.org/deeplinks/2008/10/mccain-campaign-feels-dmca-sting.

35. Lwin Aung Soe, ''Request Mail from Irrawaddy Website Due to Cyber Attack; Hoping to Defeat Hackers Soon,'' Save Burma, September 19, 2008, http://antidictatorship.wordpress.com/2008/09/19/request-mail-from-irrawaddy-website-due-to-cyber-attack/.

36. Irrawaddy system administrators, e-mail message to author, May 2008.

37. Citizen Media Law Project, ''Colocation America v. Garga-Richardson (Letter),'' April 1, 2009, http://www.citmedialaw.org/threats/colocation-america-v-garga-richardson-letter.

38. Vineetha Menon, ''US Sanctions Sees Live Messenger Blocked in Syria,'' itp.net, May 25, 2009, http://www.itp.net/news/556637-us-sanctions-sees-live-messenger-blocked-in-syria.

39. Brad Stone and Miguel Helft, ''In Developing Countries, Web Grows without Profit,'' *New York Times*, April 26, 2009, http://www.nytimes.com/2009/04/27/technology/start-ups/27global.html.