The New Gatekeepers:
Controlling Information in the Internet Age

A Report to the Center for International Media Assistance

By Bill Ristow

April 17, 2013

CIMA Center for International Media Assistance

NED National Endowment for Democracy
Supporting freedom around the world

The Center for International Media Assistance (CIMA), at the National Endowment for Democracy, works to strengthen the support, raise the visibility, and improve the effectiveness of independent media development throughout the world. The Center provides information, builds networks, conducts research, and highlights the indispensable role independent media play in the creation and development of sustainable democracies. An important aspect of CIMA's work is to research ways to attract additional U.S. private sector interest in and support for international media development. The Center was one of the of the main nongovernmental organizers of World Press Freedom Day 2011 in Washington, DC.

CIMA convenes working groups, discussions, and panels on a variety of topics in the field of media development and assistance. The center also issues reports and recommendations based on working group discussions and other investigations. These reports aim to provide policymakers, as well as donors and practitioners, with ideas for bolstering the effectiveness of media assistance.

Marguerite H. Sullivan
Senior Director

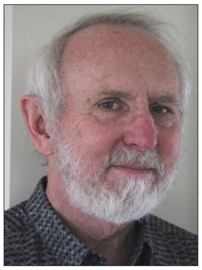
Center for International Media Assistance
National Endowment for Democracy
1025 F Street, N.W., 8th Floor
Washington, DC 20004

Phone: (202) 378-9700
Fax: (202) 378-9407
Email: CIMA@ned.org
URL: http://cima.ned.org

Design and Layout by Valerie Popper

About the Author

Bill Ristow



Bill Ristow is a journalist and international journalism trainer based in Seattle, Washington. After a 23-year career at the *Seattle Times*, where he held positions including metro editor and features editor, he has trained professional journalists and students in Uganda, Ethiopia, and Kenya, and, most recently, as a Fulbright Scholar at the University of Ghana. He has authored four other reports for CIMA: *Sword and Shield: Self-Regulation and International Media* and *Under Attack: Practicing Journalism in a Dangerous World*, both published in 2009; *Cash for Coverage: Bribery of Journalists Around the World*, published in 2010; and *Independent Media in Exile, published in 2011*.

Table of Contents

Preface

The Center for International Media Assistance (CIMA) at the National Endowment for Democracy commissioned this study of how the technological revolution of the past few decades is transforming large, Internet-based corporations into the new gatekeepers of news and information. The report examines these corporations' policies and practices and looks at the work of a growing number of academics, civil-society organizations, and advocacy groups attempting to monitor the impact of these new information gatekeepers.

CIMA is grateful to Bill Ristow, a veteran journalist and journalism trainer, for his research and insights on this topic. We hope that this report will become an important reference for international media development efforts.

Marguerite H. Sullivan
Senior Director
Center for International Media Assistance

Executive Summary

The technological revolution of the past few decades has opened up a world of information for anyone with a computer, smartphone, tablet, and an Internet connection. And it has created a new corporate world as well: companies that didn't exist 20 years ago but that have become among the most highly capitalized in the world by creating ways to help us work, play, converse, learn, argue, shop, and do nearly anything else, all online.

In the process, whether by helping us find information, organize it, prioritize it, or share it, in many ways these Internet companies have become the new gatekeepers of information–and their data-parsing algorithms the twenty-first century equivalent of the stereotypical editor with the green eyeshade who filtered the news before passing it along to readers.

Of course, there are many big differences between that editor and, say, Google, Twitter, or Facebook. But one of the biggest is that these new gatekeepers aren't just working in a single newsroom in a single city, largely isolated from everyone else. The Internet companies, though the largest of them are based in the United States, are literally working on the World Wide Web, playing on a global scale and hoping to elbow out their competitors to lock up rich international markets.

As they have expanded globally, these pioneering corporations have had to face, and deal with, a tough reality. The Internet that gave them birth espouses all sorts of high-minded principles of open and free expression. But many of the governments in countries that offer tantalizingly large commercial markets not only don't espouse those principles, they actively deny them.

And so the computer and software engineers who have taken us out into the world increasingly find themselves having to navigate its thorniest problems, balancing profit against human rights, and thinking about hate speech, censorship, and yes, whether an image of a woman breastfeeding her baby violates a policy against depicting nudity.

As they forge ahead, a growing number of academics, civil-society organizations, and advocacy groups are working to monitor the impact of the new information gatekeepers. They appreciate the challenge these companies face and laud them for much that they have achieved. But they also argue articulately that more oversight, more transparency, is needed.

And they point to the companies' own principles. Google, for instance, has long been known for an informal motto from its early days, "Don't be evil." Given that, "it's difficult to do business in a country that doesn't have

that principle," said Madeline Earp, Asia analyst at Freedom House. When it comes to the thorny issues of free flow of information, she said, "companies themselves cannot be the final arbiters, which they are by default right now."[1]

Colin Maclay, managing director of the Berkman Center for Internet and Society at Harvard University, makes a specialty of studying such things. "Can we get the Internet companies to set a standard? Do we know what good behavior looks like?" he wonders.

"If we can set global norms about what's good behavior and what's not, then we're hopeful that in some of those challenging markets we can have better outcomes."[2]

This report offers these recommendations for addressing the role of the new information gatekeepers in the age of the Internet:

- **The dominant Internet companies should be more transparent about how they decide on content issues.** It's not enough to tell users, in effect, "trust us." Without violating legitimate proprietary concerns, there is certainly room for a more publicly visible form of internal review covering how these corporations are interacting with countries around the world in making their gatekeeping decisions.

- **The start-ups of today should consider the lessons of the recent past.** If we've learned anything in watching the current tech revolution, it is that we shouldn't assume that the companies on top today will be on top tomorrow. "I hope that the next generation of companies that's forming now has something akin to privacy and transparency in their mission statement," Maclay said, "hard-baking it in the beginning, realizing that they're going to be facing challenges, from governments, from gatekeeping functions."

- **Twitter (and the telecoms, and other ICT companies) should join the Global Network Initiative.** The initiative is still in its formative years. But its strong set of principles and a collaborative approach involving human-rights groups, ICT companies, academics, and investor groups holds great promise. One of its biggest weaknesses is that it has so far only attracted three of the biggest Internet names: Google, Microsoft, and Yahoo. They are big names indeed–but without a much broader industry base, GNI will have trouble growing into the powerhouse it should become.

- **The Global Network Initiative should toughen up**. Considering the challenging nature of its goals and the range of highly diverse participants, the work GNI has done in launching itself is highly laudable. But it has been more than three years since its launch, and if the organization means what it says about its long-term mission, it must move at least to require a more transparent process with its assessments of the big corporate participants.

Prologue

Back in the olden days–that would be all of 20 or 25 years ago–it was so innocently simple. If we wanted news or information–about our neighborhood, our country, our world–we had just a few choices. We could turn to a local newspaper, or to a national magazine, or a radio or television station, and the professional descendants of Walter Cronkite would calmly and authoritatively tell us "the way it is."

This applied whether we were in a democratic society (where the role of those journalists was benign, if not always wholly unbiased) or in repressive states (where the news could be controlled based on government dictates).

Think of these people as guarding the gate in a tall wall. On one side of the wall, in a gigantic, unruly, and rather scary territory, was *all the information in the world*, swirling chaotically. On the other side? All of us. We only wanted bits and pieces of all that information, and probably had little idea of what was out there. The journalists, we understood, would study everything, filter most of it, and then package it in a safe, tidy way before allowing it through to our side.

The Internet, as famously remarked at the time, is like the world's biggest library–but all the books have fallen onto the floor.

They were the "gatekeepers." And whether or not we trusted them, for many years they satisfied our perceived needs. Until one day it all changed. Welcome, Internet.

It's not that there was an explosion, although the result was the same. Rather, it was as though the gate and all the walls quietly dissolved. It took the gatekeepers a surprisingly long time to realize it, but suddenly, there was nothing, really, between all of us … and all that liberating, messy, contradictory, energizing, amazing information.

A newly enabled populace reveled in this new world. We waded in, rummaged through all that information, laughed at the gatekeepers. Never again! we cried out. From this day and forevermore, information is free! Each one of us can choose what he or she wants, and nobody–not a stuffy editor, not an authoritarian dictator–can keep us from what is rightfully ours.

Except for one thing. The Internet, as famously remarked, is like the world's biggest library–but all the books have fallen onto the floor.[3] The gates may be open, the walls may be down. But sorry, everyone; we still need gatekeepers.

Soon enough, they came along–just in a different form, to fit the new environment. They have variously been termed "the sovereigns of cyberspace" or, as one of the new gatekeepers modestly describes itself, "the free speech wing of the free speech party." Whatever you call them, one thing is clear: We still haven't sorted out all the implications, especially for free expression and human rights around the world.

Sovereigns? Or Salvation?

It was not just the Internet that changed everything, of course. Just as important was the technological tectonic shift that made the Internet possible: the digitizing of everything, from words to sounds to photos to video. That revolution freed information from the confines of print or vinyl or celluloid, making possible the new distribution channels that can send it anywhere in the world in a matter of moments.

But there is a darker side to digitization. At one and the same time it liberates information–and makes it possible to spy on it, to track it, to control it, to manipulate it in ways never possible before. And it leaves effective control of all these things not just in the hands of governments, but more and more, in the hands of the computer engineers and corporate executives who have turned ambitious little startups into some of the most powerful and highly capitalized companies in the history of business. (Taken as a group, and including telecommunications as well as Internet companies, they are known as the information and communications technology industry, or ICT.) This is why Rebecca MacKinnon, a senior fellow with the New America Foundation, in her book, *Consent of the Networked*, terms these ICT companies and their leaders "the sovereigns of cyberspace."

It used to be that "sovereignty over our physical freedoms or lack thereof was controlled almost entirely by nation-states," MacKinnon said in a TedTalks presentation outlining the thrust of her book. "But now we have this new layer of private sovereignty in cyberspace, and their decisions about software coding, engineering, design, terms of service all act as a kind of law that shape what we can and cannot do with our digital lives."[4]

This matters, MacKinnon said, because "in more and more countries the relationship between citizens and government is mediated through the Internet, which is comprised primarily of privately owned and operated services."

The large corporations that have had the greatest success in this new world–Google, Twitter, Facebook, and Yahoo–all take often admirably strong public stances in support of openness and other high principles. Twitter is proud of calling itself "the free speech wing of the free speech party." Google has long been known for an informal motto from its early days, "Don't be evil."

But MacKinnon, and many others working on issues of free expression, privacy, and Internet governance, argue that simply espousing high principles isn't enough, and that the significance of these corporations' role in managing information demands some formalized system of accountability. By no means is there widespread agreement about this within the industry, and even among advocates, there's no final consensus on what form this accountability should take. But the resolve is clear.

Colin Maclay, managing director of the Berkman Center for Internet and Society at Harvard University, described the challenge the new Internet companies face when they try to conduct business in less than democratic countries.

"Companies know that resisting a government is costly, perhaps placing their operating license and local employees at risk, but that acceding blindly can have terrible implications for them and their users, and that this tension is ever more part of their business," he wrote. "A (more) sustainable solution is essential."[5]

That solution, Maclay argues, will require corporations "to meaningfully integrate the protection of freedom of expression and privacy into both business practice and corporate culture."

Some of the largest of the ICT companies have taken major steps toward that sort of commitment, prodded, sometimes, after embarrassing blunders brought them unwanted international human-rights attention in the past decade. But for all of their passionate defense of an open Internet and their proclamations about free and open discourse (especially on their platforms), they remain companies often in competition with each other for market share and advertising dollars and responsible to shareholders for growth and profit. Perhaps as a result, outside observers often say that these companies' transparency about themselves–including particularly how they navigate the challenging waters of international human rights in the era of the Internet–has considerable room for improvement.

One of those observers is Tarleton Gillespie, an associate professor in the Department of Communication at Cornell University, who has intensively studied how the policies and actions of Internet companies affect the flow of information around the world.If he were talking to a gathering of ICT executives, Gillespie said, he would try "drawing their attention to their own public role–and how that tangles them with this sort of longer history of providing information to a public, and the problems and pitfalls that can present."

He would talk about the "big consequences" of the things they do, both the technical things such as algorithms, and the policies they draw up.

He would tell them, he said, that it is all about their "public obligation."[6]

Gatekeepers and Gated in a Networked World

“Gatekeeping,” as classically defined by Syracuse University professor Pamela Shoemaker in 1991, “is the process by which the billions of messages that are available in the world get cut down and transformed into the hundreds of messages that reach a given person on a given day.”[7]

In talking to his students, Gillespie said, he noticed that while they seemed aware of how information was being filtered through gatekeeping in the traditional media, they were surprised when he said Google was doing that, too. And at first glance, that makes sense. All the “gates” are gone, after all, so how can you compare what a company like Google does to the job of a newspaper editor?

Indeed, Google would prefer you *didn’t* make that comparison. “I understand where that gatekeeping concept comes from, but honestly, it’s not one that we totally agree with,” said Christine Chen, a senior manager for free expression and international relations at Google. Instead, she and others at Google simply want to say that their “core mission is to organize all the world’s information.”[8]

But it’s certainly the case that Google and its peers are gatekeepers, said Karine Nahon, an associate professor in the Information School at the University of Washington, who has made a specialty of studying “network gatekeeping,” as she calls the new processes.

She starts by acknowledging that there *is* something very new going on. “The role of the gated–the person who is subject to control–has changed enormously over the past 20 years. Each one of us can be a gatekeeper today. When I decide what to display on my screen, I’m a gatekeeper.”[9]

But in this new environment, where there is so much information, so widely scattered, we rely on the new network gatekeepers, the large technology companies whose products let us move around the Internet. These companies–whether Google or Yahoo, Facebook or Twitter, China’s Sina Weibo or Russia’s VK–“regulate the structure, the information tools, and a lot of time that affects what we learn, how we behave,” Nahon said. And in that sense, simply by providing the tools for us to organize and wander through cyberspace–and particularly, by the way those tools work–they have powers far greater than the newspaper editor.

A search engine is certainly a gatekeeper, Nahon said, because it is “prioritizing information for you. Whatever they give us on the first page, this is what you’re going to digest.” Even a search engine’s autocomplete function, which starts suggesting search terms for you as soon as you type in a few letters, fits her definition: “Contextualizing is definitely a gatekeeping mechanism.”

Network gatekeeping involves much more than search, however. The big technology companies (or, often, the disembodied software that automates much of what they do) are making decisions every day about just what pieces of that enormous global pile of information they will allow users to see.

Consider:

- A journalist at the London Olympics, critical of NBC's coverage, shared the corporate email address of a network official with his Twitter followers. Twitter, which was engaged in a partnership with NBC, suspended his account, blocking his tweets from view.[10]
- Mark Fiore, the first editorial cartoonist to win a Pulitzer for purely online work, submitted an iTunes app featuring his cartoons; Apple rejected it, saying "it contains content that ridicules public figures," in violation of the company's standards.[11]
- After NASA posted material on YouTube of Curiosity landing on Mars last year, one video was abruptly taken down–with a message saying it had been blocked due to copyright issues, even though NASA videos were clearly publicly owned.[12]

All these actions were reversed (after the glare of negative publicity), and none amounted to much more than an online stumble, although they demonstrate how easily whims or mistakes can "gatekeep" material right out of cyberspace. But there are considerably more troubling examples of ways the free flow of information can be interrupted by the platforms themselves.

Last year in Hungary, a far-right politician asked for a list of Jews in the government who might pose "a security risk." A group started a Facebook page to publicize a protest against his effort, and organizers asked protesters to wear a badge bearing the word "Jude," as was required in Nazi Germany.

The page was removed from Facebook, apparently by an automatic tool meant to filter hate speech, or content that could be inciting in nature. "The policy makers of Facebook almost certainly did not intend to block the anti-fascists' right to use Nazi-style Jewish badges on the internet to fight against neo-Nazis," said an article from the Oxford-based organization Free Speech Debate. "But it shows the perils and capriciousness of automated content regulation."[13]

When Facebook banned a page for the word "Jude;" when Apple rejected a cartoonist's work for doing what editorial cartoonists very publicly do every day; when YouTube removed a video posted by a public agency on the basis of a mistaken copyright claim, they were all relying on policies or practices they had developed in good faith but that failed to meet the demands of a rapidly evolving information world.

Much of the online gatekeeping, in democratic and non-democratic states alike, uses computer algorithms–programs that use mathematical formulas to analyze and select from large masses of data. Because they've become so important in the flow of information, people who study and teach about journalism have to take them into account, and Gillespie, at Cornell, has made them one of his specialties.

Algorithms, he has written, "not only help us find information, they provide a means to know what there is to know and how to know it, to participate in social and political discourse, and to familiarize ourselves with the publics in which we participate."[14]

Companies such as YouTube, Gillespie says, are "being pushed into a situation where they are arbiters on a number of tricky issues" such as free speech and incitement to violence. These companies "wanted to curate [the public discussion], but not necessarily have the responsibility" or know how to handle it, he said. And he added that he's not sure "the degree that people in these sites think of themselves as the hosts of public discourse."[15]

Gillespie sees two main ways the companies approach their curating role. One way involves looking at every item in advance. This is what Apple does in reviewing potential apps, and it led to the initial rejection of the editorial-cartoonist app. Gillespie calls Apple "an extreme in the proactive approach."

Alternatively, companies can allow things to be posted, and then have a "flagging" process allowing others to object, leading to some form of review and possible removal. That's what happened at YouTube when the NASA video was mistakenly and temporarily taken down: someone wrongly flagged it. Gillespie calls this "flagging" approach "a 'better than not' solution," and thus a fairly popular one.

He's still exploring what he calls a possible third way: "Can we come up with a technical solution that's more sophisticated?" Would it be possible, he wonders, to "tag," or electronically mark, content in a sophisticated enough way that users could set up their own filters, self-selecting not to receive material objectionable to them while allowing others to see it? He's not sure, calling balancing community values against the protection of speech an "almost intractable" problem.[16]

Policies, Terms of Service…and War

All of the major ICT players have documents (variously called policies, terms of service, guidelines, or rules) that describe the things the individual platform will or will not allow and, sometimes, what they will do about it and how.[17]

Some of the policies are relatively simple and non-controversial. Everyone bars child pornography or copyright violations, for instance. It can get more complicated as you move into the more nuanced aspects of speech. Facebook's rule against content that contains nudity, for example, caused it to block a *New Yorker* cartoon of Adam and Eve with her nipples visible from the magazine's Facebook page in 2012.[18]

This was actually the second confrontation between Facebook policies and women's breasts in the same year. Earlier, a widespread public protest about the blocking of some breastfeeding photos on women's pages caused the company to clarify that it would allow photos of breasts unless "the child is not actively engaged in nursing."[19]

The tone of the policies may provide a glimpse at the individual company's approach. In "The Twitter Rules," that service states: "We respect the ownership of the content that users share and each user is responsible for the content he or she provides. Because of these principles, we do not actively monitor user's content and will not censor user content, except in limited circumstances described below."[20]

Apple, meanwhile, in an introduction to guidelines for submissions to the App Store, comments that the company views apps "different than books or songs, which we do not curate. If you want to criticize a religion, write a book. If you want to describe sex, write a book or a song, or create a medical app. It can get complicated, but we have decided to not allow certain kinds of content in the App Store … We will reject Apps for any content or behavior that we believe is over the line. What line, you ask? Well, as a Supreme Court Justice once said, 'I'll know it when I see it.' And we think that you will also know it when you cross it."[21]

Well, maybe not *everybody* will know. *Wired* magazine reported in August 2012 about the App Store's rejection of an app mapping the location of every U.S. drone strike around the world, based on public media accounts. *Wired* quoted the final rejection email: "We found that your app contains content that many audiences would find objectionable, which is not in compliance with the App Store Review Guidelines."[22] The American Civil Liberties Union, critical of the action, remarked, "An app providing a stream of basic information about the conduct of a policy that is the subject of current public debate would seem as American as, uh, apple pie."[23]

Interpreting and enforcing the various policies and rules can get especially tricky in the heat of war, especially when both sides are using social-media platforms to promote their positions. When that happened during the fighting between Hamas and the Israel Defense Forces (IDF) in Gaza in November 2012, it provoked thoughtful analysis of the position the social media found themselves in on the front line. “The clash has highlighted the tensions companies face between freedom of speech and violence, how the Internet has become a battleground for public opinion, and the role of the public in negotiating conflict,” wrote the group Global Voices Advocacy.[24]

In the midst of the conflict, the IDF and Hamas traded tweets that could be interpreted as threatening or merely taunting, depending on your perspective; and placed graphic video images of attacks and killings on Facebook and YouTube. The problem: the terms of service of those Internet companies could easily be seen as barring pretty much everything that was posted, *BuzzFeed*’s Matt Buchanan noted, citing specific examples:[25]

> Twitter, for instance, bans “violence and threats”: “You may not publish or post direct, specific threats of violence against others.” … YouTube’s community guidelines warn, “Graphic or gratuitous violence is not allowed. If your video shows someone being physically hurt, attacked, or humiliated, don’t post it.” …Facebook’s terms say, “You will not post content that: is hate speech, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence.” …

Buchanan concluded that “so far,” at least, what the platforms did was proper. “It’s brutal, it’s propaganda–it’s *war*–but it’s also important,” he wrote. “I suspect this is precisely why these social networks, despite the apparent violation of their terms of service, are leaving this stuff up. We’re witnessing a country and its opponent document their own war against each other in real time. This has never been done before, not like this. Good, bad, or ugly, this shouldn’t be pulled from the light of day.”

For some, though, questions of transparency remain.

Mathew Ingram, writing on GigaOM, agreed that “it’s a great thing to have all these sources of information.” But, he added, the Gaza events highlighted “just how much of our perception of such a conflict comes to us through proprietary platforms like Twitter and Facebook and YouTube. What duties or responsibilities do they have (if any) to monitor or regulate that information?”[26]

The lack of explanation, Ingram said, “reinforces the same problem that has arisen before with Facebook and other similar social networks as a platform for speech: namely, they are effectively a series of black boxes when it comes to decision-making around what gets removed … And while they have all expressed their commitment to free speech in some form or another, they have absolutely no obligation to uphold that, or to tell users when information has been removed, or why.

“We may have disrupted our old information gatekeepers–newspapers, television, even governments–but in many ways we have just exchanged them for shiny new ones. And they are just as inscrutable, if not more so.”

Navigating Turbulent International Waters

If the Internet as information-distributor can create "intractable" problems even in democracies, a growing number of people are warning that online issues have become a matter of urgent concern in states that are less than democratic. The concerns have caused some people to raise a sort of "be careful what you wish for" admonition about the Internet.

One of the sharpest tongues in this regard belongs to Evgeny Morozov, a contributing editor for the *New Republic*, whose book, *The Net Delusion: The Dark Side of Internet Freedom* was published in 2011. Scoffing at "cyberutopians," he asks, "What if the liberating potential of the Internet also contains the seeds of depoliticization and thus dedemocratization?"[27]

Free-speech advocates have similar worries about the hazards of the online world. "By 2009, over half the journalists imprisoned for their work globally wrote for the Internet," said Danny O'Brien, then the Internet advocacy coordinator with the Committee to Protect Journalists.[28]

"If you want to make the point as bluntly as possible, governments like to clamp down on people's speech," said Eva Galperin, international freedom of expression coordinator for the Electronic Frontier Foundation (EFF). In this regard, she said, "the Internet is a double-edged sword." Yes, it provides a remarkable vehicle for the flow of information. But it also "allows for a level of tracking, censorship and surveillance that's never been seen before. I would say at the moment it's a draw."[29]

A "draw," perhaps but it's hard not to be sobered by the trends documented in the *Freedom On the Net 2012* report prepared by Freedom House:[30]

- 42 percent of the 47 countries covered in the report have had a "negative trajectory" on their Internet freedom scores since the previous Freedom House report.
- 40 percent have passed new laws or regulations "that could negatively affect free speech online."
- In 55 percent, a blogger or other similar content-producer was arrested for online or mobile content.
- In 30 percent of the countries, paid pro-government commentators are posting online, only rarely identifying themselves.
- In 40 percent, a blogger or other similar content-producer was physically attacked or killed.

That tally "is one of the key reasons not to just sit back and assume that the Internet will make us free," said Madeline Earp, who joined Freedom House as Asia analyst for its Freedom on the Net project in 2012 after working on Asia/China issues with the Committee to Protect Journalists (CPJ) for a number of years. "You can't deny that there are huge positive movements underway. But when you look on balance, that's trickier."[31]

It is happening, really, everywhere. In Iran, the entire Gmail system was shut down in February 2010.[32] During protests in Bahrain in 2011, the government blocked specific YouTube accounts and videos.[33] In the United Arab Emirates, security services demand Facebook passwords from political prisoners.[34] In India, faced with a court order, Google and Facebook removed content "considered religiously offensive" from local websites.[35] In Australia, a police commissioner met with a Facebook official "over his concerns the site's users incite hatred and undermine the criminal justice system."[36]

This is the global environment where network-gatekeeping companies such as Google, Facebook, Yahoo and Twitter want to operate–where they *need* to operate, as commercial businesses, to maintain their positions in the world economy. So how do they navigate the turbulent waters?

There has been a lot of trial-and-error learning, punctuated by false starts, embarrassing gaffes, heated confrontations, and delicate negotiations. And it has provided a lot of work for international lawyers.

An excellent inside look at how Google and its lawyers carry out the process of vetting controversial user-generated content was published in the *New York Times Magazine* in 2008. The author, Jeffrey Rosen, a law professor at George Washington University, talked with Google employees who rule on the content, and also "decide what controversial material does and doesn't appear on the local search engines that Google maintains in many countries in the world, as well as on Google.com." These people, Rosen writes, "arguably have more influence over the contours of online expression than anyone else on the planet."[37]

Twitter found itself in the midst of a combination gatekeeping and international-politics incident immediately after the 2009 Iranian elections, when the short-messaging service was being widely used by Iranian activists involved in protests and by the Western media who were following them. When a State Department staffer approached Twitter, asking it to delay its scheduled worldwide system maintenance to avoid cutting off the Iranian traffic, the social-media service complied, in recognition of "the role Twitter is currently playing as an important communication tool in Iran."[38]

And Facebook was forced to scramble in Syria in 2012, when a young woman, Dana Bakdounis, posted a photo of herself without her state-required veil. Bakdounis's post quickly provoked controversy in Syria, and suddenly it was missing–removed by Facebook administrators. Facebook restored the page after several days, and acknowledged in a statement having made "multiple mistakes over a number of days" that delayed its fix. "Mistakes aside," as the BBC commented, "the allegations alone have raised interesting questions about the non-formalised and seemingly omnipotent role that one of the best-known social media channels plays in this process of intense regional change and upheaval."[39]

Perhaps the best-known example of a global company feeling its way in the midst of a conflict of standards was the controversial "Innocence of Muslims" video. With violent reactions taking place throughout the Arab world, Google decided on its own, in September 2012, to block in Egypt and Libya the video from its YouTube subsidiary. Google acknowledged the decision was unusual; normally, it would only block content that it determined was hate speech, or in response to a legitimate court order or government request. Neither of those things applied, Google said, but the killing of four American diplomats in Libya justified the action.

"Google's action raises fundamental questions about the control that Internet companies have over online expression," wrote reporter Claire Cain Miller in the *New York Times*. "Should the companies themselves decide what standards govern what is seen on the Internet? How consistently should these policies be applied?"[40]

The article quoted Peter Spiro, an international law professor at Temple University: "Google is the world's gatekeeper for information so if Google wants to define the First Amendment to exclude this sort of material then there's not a lot the rest of the world can do about it." Spiro added that he "provisionally" supported what Google had done.

MacKinnon, author of *Consent of the Networked*, is also inclined to support Google's actions, noting that the video was quietly restored to YouTube in Egypt and Libya after less than three weeks. She was glad that Google "didn't allow it to turn into a precedent more broadly. Clearly they agonized over the decision, and they did what they thought was right."[41] But she strongly believes that when content does or does not get taken down in this sort of controversial setting, the companies should "do more to clarify the process. It would be very interesting to know what their internal post-mortem was." Google representative Christine Chen said the company declined to comment on post-mortem conversations, saying only that "the decision was not one that we took lightly, and was due to the grave situation on the ground."[42]

Dealing With Governments: Takedown Requests

Every day–or more accurately, every hour of every day–someone, somewhere, is asking (or demanding) that one of the Internet platforms remove some piece of content.

The overwhelming majority of these "takedown requests" are from copyright owners or their representatives, who have seen their material improperly made available on the Internet. On a single, random day in March 2013, Google reported having received 78 different copyright-related takedown requests, asking the company to "remove search results that link to allegedly infringing content."[43] The requests were for removal of as few as one single URL link, to as many as 7,987 URLs specified in one request (nearly all from a domain based in the Netherlands).

Google took a pioneering step when it began publicly releasing reports about all the times it is asked to remove content from one of its products, dividing them into copyright issues (by far the most numerous) and requests from governments or courts. The first transparency report covered the period July through December 2009, and the reports have become more detailed and sophisticated in the years since.[44]

Copyright requests may be voluminous, but it is the request from governments and courts that raise the greatest concerns for free-speech advocates, who have overwhelmingly praised Google as a groundbreaker in its transparency. (Google has since been joined by several others, notably including Twitter, LinkedIn, and Microsoft and its subsidiary Skype.) In a blog post earlier this year, EFF's Galperin commented, "These reports have provided an invaluable source of information about the extent of law enforcement access to private data, and we commend these companies for collecting and publishing them."[45]

The reports on government requests include compliance statistics–how often Google provided what was asked for. Those statistics show that Google's compliance with all government requests has declined from 76 percent in the period ending Dec. 31, 2010, to 52 percent in the period ending June 30, 2012.

The reports include "Notable observations" on a country-by-country basis. For example, in a recent report the entry on France includes: "In response to a court order, we removed 992 search results that allegedly violated the privacy of an individual." But it also states, "We received a request from legal representatives of a former politician to remove a blog post that allegedly defames him by explaining his connections with the pharmaceutical lobby. We did not remove the blog post."[46]

Beyond complaints about very individual cases, the Internet companies also must deal with general content that may conflict with laws or norms of specific countries. The "Innocence of Muslims" affair was one such, and in addition to unilaterally removing the video in Egypt and Libya, Google's YouTube subsidiary also removed it on court order in a number of other countries.

Twitter adopted a policy allowing it to block content in this "country-specific" way early in 2012, and then used that policy for the first time in October that year at the request of local authorities, making it impossible for German users of Twitter to see posts by a neo-Nazi group banned under German law.

"Twitter has little choice when ordered to comply with local laws," said an article in the UK newspaper *The Independent*. "Its country specific blocking is an attempt to limit any damage done in the minds of those who would rather see the site place freedom of speech above local censorship laws." And the article quoted a tweet from Twitter's lawyer, Alex Macgillivray: "Never want to withhold content; good to have tools to do it narrowly & transparently."[47]

The Electronic Frontier Foundation produces annual reports intended to help users evaluate Internet companies on their policies and practices concerning government requests for information. The "Who Has Your Back" ratings for 2012 covered 18 major companies, examining "their terms of service, privacy policies, and published law enforcement guides, if any … [and] their track record of fighting for user privacy in the courts," among other things.

Each company is rated in four categories, receiving a full star, half star, or no star in each one. In 2012, for example, Twitter received three full and one half stars; Google two full and two half; and Yahoo, Microsoft, and Apple one full star apiece. And the report praises the industry overall for significant improvements over the previous year.[48]

The EFF campaign focuses primarily on relationships with the U.S. government, laws, and courts. But as several observers have argued, it is a critical first step to institutionalize these sorts of policies and standards within the United States, where most of the companies are based, because that will make it far more likely they will take them overseas.

How the companies act overseas, meanwhile, remains very much a work in progress.

Jason Pontin, editor in chief and publisher of the *MIT Technology Review*, tackled the complexities of this issue in February 2013 in a sweeping essay addressing "the limits of what may be shown or said on the Web."[49]

After describing a number of international incidents, including the “Innocence of Muslims” affair, Pontin commented, “American Internet companies have proposed a sunny compromise. To governments whose understanding of free speech departs from the American standard, they have promised: we will comply with local laws. To communities convinced that hateful expression *is* harmful, they’ve said: we will censor hate speech.”

He described this compromise as “a hack designed by Silicon Valley’s engineers and lawyers to allow different legal and cultural conceptions of what may be expressed to coexist on sites used all over the world. But it has been a fidgety hack, requiring awkward accommodations.”

Pontin’s conclusion: “Because free speech is so important, and because the Internet will continue to amplify its expressions, U.S. Internet companies should apply a consistent standard everywhere in deciding what they will censor upon request.”

He takes an absolutist position in that respect. His piece, structured as a letter to the British political philosopher John Stuart Mill, concludes:

“The only principle I can imagine working is yours, where ‘harm’ is interpreted to mean physical or commercial injury but excludes personal, religious, or ideological offense. The companies should obey American laws about what expressions are legal, complying with local laws only when they are consistent with your principle.”

When that’s not the case, he said, they should “refuse to operate inside a country.”

Galperin of EFF tends to support that tough stance, though with some equivocation.

“Anyone who says they are ‘the free speech wing of the free speech party,’ as Twitter does, needs to be extremely circumspect about where they put their offices”–which includes sales offices, she noted.

Taking material down only in specific countries, she said, is “the least worst solution.” And while she would prefer that the companies stand up for free speech, even if it means not having an office in a certain country, “we understand the commercial pressures.”[50]

China: Formidable Presence, Uncertain Future

With a population of more than 1.3 billion and a well-developed technological infrastructure, China was a natural commercial target for U.S.-based tech companies needing to expand their markets, and they dove in with a vengeance. But it is also a country with one of the worst freedom of expression records in the world, presenting those companies with a stark dilemma: Could they square their business interests and desires with their corporate standards, Western human-rights principles, and the Internet's own structural belief in a free and open network?

It turned out to be a dilemma with no tidy, middle-ground solution, and several of the largest corporations were accused of missteps during the early years of trying to make things work. But it was a firestorm surrounding Yahoo that made everyone from human-rights advocates to members of Congress sit up and take notice.

With a population of more than 1.3 billion and a well-developed technological infrastructure, China was a natural commercial target for U.S.-based tech companies needing to expand their markets.

In 2002 and 2004, two Chinese activists were jailed for allegedly subversive activities based on their writings on Yahoo message boards. China demanded e-mail records and other identifying material for both–and Yahoo turned them over.

Initially, Yahoo co-founder Jerry Yang flatly defended the company's actions. "To be doing business in China, or anywhere else in the world, we have to comply with local law," he said in 2005. "We don't know what they want that information for, we're not told what they look for. If they give us the proper documentation and court orders, we give them things that satisfy both our privacy policy and the local rules."[51]

That stance didn't last. Yahoo eventually retreated, apologized to Congress for not fully sharing information on the debacle, claiming it was due to a "misunderstanding," and it has gone on to radically overhaul its approach to human-rights issues. But the repercussions of the affair made crystal clear not only to Yahoo, but to everyone else tiptoeing in the waters of the Chinese Internet market, that they needed to be on their guard.

China became more aggressive roughly five years ago. The country's "censorship machine has been operating ever more efficiently since mid-2008," according to a *New York Times* report, "and restrictions once viewed as temporary–like bans on Facebook, YouTube and Twitter–are now considered permanent."[52]

Google closed its search operation in China in 2010, due to extensive filtering of results. Chinese users were still generally able to access the company's Hong Kong server, but when searches there were also subjected to filtering, Google began, in May 2012, putting up a notice advising users of the tactic whenever it was spotted. China responded by blocking all access to Google for 24 hours and increasing censorship of Gmail messages; eventually, in December 2012, Google stopped posting the notices.

"Every move Google has tried to make to combat, expose or pervert China's efforts at censorship has been met and defeated by the authorities–often with overwhelming force," said an article in the *Economist* early this year. "In the end, it may be that Google simply stopped banging its head against the wall, having realized that the headache was pointless."[53]

Meanwhile, China was also developing its own local search and social-media companies, governed by Chinese regulations (see box). This was part of what Danny O'Brien, then of CPJ, described as a two-pronged approach. First, the government developed a sophisticated technological and censorship apparatus, generally known as the "Great Firewall," that O'Brien said "surprised" many people in its ability to block the traditional Internet. Second, while allowing local companies to capitalize on the huge market available through the internal network, the government has dictated a sort of corporate "self-discipline" in which companies use their own staff and technology to monitor the "wrong sort of message."[54]

This has raised challenging issues for China, O'Brien noted. It is hugely expensive to maintain the technological structure; it has created continuing internal fights about who controls the Great Firewall; and it has placed enormous burdens on the private companies (some of them traded on international stock markets), both because of the special requirements inside China, and the special challenge if they want to expand outside of China because of the different technical systems.

As a result, he said, the situation for the Chinese government is "a bit like balancing on a unicycle," trying to keep the Internet within China "from falling into its natural state, which is sort of everybody talking to each other."

Elsewhere in the World…

Google, Facebook, Twitter and other U.S.-based companies are by no means the only corporate players filling some aspects of a gatekeeping role. The Russian-language social media site VK.com (formerly VKontákte, meaning "In Touch," or "In Contact") is approaching 200 million registered users and is among the top 25 Internet sites in the world in traffic, according to the Web information company Alexa.[1] Mixi.com is at least competitive with Facebook in Japan,[2] while in South Africa mobile-based site mxit.com is well ahead of Facebook, according to CNN.[3]

But by far the largest non-U.S. Internet companies are based in China, which has a particularly rich and active homegrown Internet and social-media scene. They include the giant search engine Baidu; several instant-messaging or chat services; specialty sites focusing on, for example, literary or cultural topics; and the big "weibos," or microblogs–similar to Twitter in using a 140-character limit, but much more flexible because Chinese characters carry far more information than Western alphabets.

Endnotes

1. http://www.alexa.com/siteinfo/vk.com..

2. David Cohen, "9 countries stand between Facebook and global domination," AllFacebook, http://allfacebook.com/facebook-world-domination_b75339, January 26, 2012.

3. Teo Kermeliotis, "Mxit: South Africa's Facebook beater," CNN, http://www.cnn.com/2012/11/07/tech/mxit-mobile-social-network/index.html, November 9, 2012.

Make no mistake, however: People *are* talking to each other in the Chinese social media. They're talking a lot, and often; they're talking in a way that can seem startlingly unfettered in their open criticism of official actions, even though censorship is very much there.

David Wertime is the Washington, DC-based editor and co-founder of *Tea Leaf Nation*, an online magazine whose staff and contributors monitor the Chinese social media from the United States and inside China, publishing articles and reports based on what they find. The purpose is partly to provide the rest of the world with a first-hand look at Chinese cultural activities, everyday life, and trends. But the magazine's writers also have a special vantage point on the state of censorship in the Chinese system.

Their primary platform for study is the social network Sina Weibo ("weibo" is the Chinese word for "microblog," and Sina is the name of the corporation that runs this particular site and several others).

The traffic on Sina Weibo can seem extraordinarily unfettered, with pointed attacks on local officials or policies interspersed with the more quotidian social-media chatter. The robustness of the conversations, Wertime said, "can be surprising and even shocking to Western observers who come on that platform for the first time. Certainly it is not free; censorship is a daily fact of life. But it is the closest thing China has to a free platform."[55]

Reports estimate as many as 1,000 censors work for Sina Weibo.[56] But Wertime and others cite research that indicates the censorship of weibos may have a pattern. If users are simply commenting on something, even to attack an official, their comments are likely to be untouched. If their posts, on the other hand, have the purpose (or result) of generating organized protest action, and especially against the central Communist Party structure, the hammer is likely to fall.[57]

Wertime said the Communist leadership may actually *like* the posts of users "venting spleen against local officials," because the central government has a strong interest in ferreting out corruption on the local level. He said people have been exposed in social media and brought down for corruption, and legal rulings have been influenced by online sentiment.

Wertime stresses that he can't guess where things will be in China in 10 years or 50 years and that it's hard to make a solid case for either optimism or pessimism. Still, he said, the scale of the social media "has already created a sense within China that certain minority opinions are more widely held than otherwise you might have expected," and that this is one of the "potentially positive, potentially quite profound long-term effects" of the weibos.

The central government, he suspects, is probably somewhat surprised at the extent of the online phenomenon in China, "and they realize they can't put this genie back in the bottle, even though technically they could flip the off switch."

He's hardly naïve, though. He points to the army of censors the weibos employ, and the even greater army of individuals paid by the government to make online postings opposing critics or supporting positions of the government, without identifying themselves–the so-called "50-Cent Party."

Madeline Earp, the China expert now with Freedom House and formerly with CPJ, said she has heard estimates as high as 2 million people being employed in the "50-Cent Party" in Beijing alone–"mind-blowing," she said, and an indication of the amount of resources the government is devoting to maintaining control of the Chinese network.[58]

She, too, feels guardedly positive, while still emphasizing areas of concern. "The microblogs have really thrown it into a starker relief," Earp said. "It's hard not to feel a sense of optimism–but you have to look at a very long-term trend. We'll be talking about the genie out of the bottle when we start seeing some officials acknowledge that this is not a practical way of managing information."

Google's executive chairman, Eric Schmidt, took an aggressive stance of his own at the start of 2013. "As the world becomes increasingly connected, their decision to be virtually isolated is very much going to affect their physical world," he said of China. "The government has to do something–they have to make it possible for people to use the internet."[59]

And what do the Chinese social-media sites think about the government's requirements that they censor content and, more recently, require real-name registration from users? It's not something they talk about publicly. But there is an intriguing hint in one highly unlikely spot: an annual stock filing to the U.S. Securities and Exchange Commission.

Sina Corporation, the parent company of Sina Weibo and others, issues a NASDAQ-traded stock. That means it must fill out the same SEC forms as anyone else. In a blog post in April 2012, Bill Bishop (a co-founder of the CBS Marketwatch program, since moved to Beijing) wrote about Sina's SEC Section 20-F filing covering the previous year–which, in a lengthy section about possible risk factors, talks about Chinese oversight.[60]

In 2012, the Chinese government demanded that microblog services start requiring real-name registration from all users, while still allowing anonymous posting. Bishop quotes from the company's SEC report, for example, that "We are required to, but have not, verified the identities of all of our users who post on Weibo, and our noncompliance exposes us to potentially severe punishment by the Chinese government." In addition, "if the Chinese government enforces compliance in the near term, such action may severely reduce Weibo user traffic." Either of those eventualities, among others, could significantly hurt the share price, the report states.

Granted, as Wertime points out in a comment on the blog, corporations commonly list any risk they can possibly think of, just to cover themselves. Still, it is fascinating to hear one of China's most successful homegrown Internet companies making its case in this particular capitalist forum.

Suppression, Yes–But New Approaches as Well

Beyond China, developments in the suppression of free expression online worry human-rights advocates. Open-Internet groups are now watching Russia more closely because of a law that went into effect in November. Ostensibly aimed at blocking child pornography, it will actually "wind up blocking all kinds of online political speech," said a report in Wired magazine. And it will allow "network providers to peer into the digital packets composing a message or transmission over a network … It allows ISPs not only to monitor the traffic, but to filter it, suppressing particular services or content."[61]

"I think Russia is definitely going to be a concern for us going forward," Earp said, with its "umbrella of state control, and given that Russia has such a bad history, especially with press freedom, and its influence on other countries."[62]

Meanwhile, some regimes are reportedly becoming more sophisticated in their approach to managing the Internet. Rather than simply trying to block offending sites altogether, governments may allow some form of controlled access–and then use it as a way of monitoring citizen behavior.

Early in 2013, for example, Iran announced that it was developing "intelligent software" to allow restricted access to officially banned social media sites such as Facebook and Twitter. Writing in the *Atlantic*, Megan Garber cited Iranian police chief Esmail Ahmadi Moghadam as saying, "Smart control of social networks will not only avoid their disadvantages, but will also allow people to benefit from their useful aspects."[63]

The "revealing" aspect of this announcement, Garber went on, was that it suggests a new sort of "strategic censorship," allowing citizens to "indict themselves" with an illusory sense of freedom. "And that is, as a strategy, very likely the future of repression–one in which access to the web won't just be the black-and-white matter of blocked vs. not, but rather something more insidious: curtailing Internet freedom by the very illusion of granting it." For similar reasons, a move by Syria to lift its ban on Facebook and YouTube in 2011 was also met with cautionary remarks from human-rights activists and even the U.S. State Department.

Quoted in the *New York Times*, Susanna Vila, of the activist site Movements.org, said, "While access to social media sites presents an opportunity for Syrians to better mobilize one another, it also makes it easier for the government to identify activists and quash protests." And Vila also said "there was growing concern that the government of Sudan was closely monitoring Facebook users there after lifting restrictions."[64]

The article also quoted a State Department official who, while welcoming "any positive steps" toward an open Internet, added, "absent the freedoms of expression and association, citizens should understand the risks."

Mobile And Telecoms: A Nightmare Ahead?

One of the concerns that can keep free-expression advocates awake at night is the importance of telephone networks in carrying Internet traffic, and the opportunity this raises for telecom companies and ministers of telecommunication to take a larger role in censorship and repression of speech.

This is particularly true with the wireless network technology built into mobile phones, which are rapidly becoming the communication mode of choice worldwide, and especially in countries where free-expression protections are problematic.

With mobile, O'Brien noted, "there's a really profound change in terms of the vulnerability of the communication. The telephone company knows who you are, where you are, controls very often the device you use."[65]

And perhaps more concerning, he said, local telephone companies "have incredibly close ties to local governments," and are often dependent on them. Sooner or later, O'Brien worries, "governments are going to realize how much material is locked up in those mobile devices … a huge stockpile of sensitive information."

Maclay, of the Berkman Center at Harvard, agrees that the telecoms "have any number of reasons why they're likely to be closer to governments, or more responsive to government regulation"–in democratic as well as non-democratic states. And, he adds, "The technology itself is so incredibly intrusive, so the opportunities [for illegally intrusive actions] are better." With people doing more and more over their mobile phones, including financial transactions, he calls it a "security nightmare."[66]

He calls the risks to privacy and security tied up in mobile phones one of "the costs of convenience. We have not yet gotten the bill, but the bill is out there waiting, and the cost is going to be substantial."

Some people are already paying the bill.

- In 2010 in India, for instance, the Ministry of Communications & Information Technology ordered all mobile telecom providers to impose a three-day ban on high levels of SMS (text) messages, in an effort to minimize unrest in anticipation of a pending high court ruling in a controversial case.[67]
- In Cambodia, the minister of telecommunication last year announced new rules regulating the use of the Internet, ordering some Internet cafes to be closed.[68]

- In Iran, the Iranian Revolutionary Guard Corps now owns a 50 percent share in that country's national telecommunication company, "effectively allowing it direct supervision on surveillance and censorship," according to an article in the *Wall Street Journal*. The article continues: "The Internet, particularly social networking sites, and mobile phones helped Iranian activists to mobilize for anti-government protests after President Mahmoud Ahmadinejad's 2009 re-election prompted allegations of voting fraud."[69]

And the *Freedom on the Net 2012* report prepared by Freedom House is littered with references to the activities of telecoms and ministries in suppressing free speech. It reports that in Bahrain, for example, all telecom companies have been required since 2009 "to keep records of customers' phone calls, emails and website visits in Bahrain for up to three years; the companies are also obliged to grant security services access to subscriber data. In 2010, those records were used against rights activists such as Abdul Ghani Khanjar, who was tortured for refusing to explain his phone discussions and text messages presented during an interrogation."[70]

Writing in his role as CPJ's Internet advocacy coordinator in December 2012, O'Brien, analyzing the just-completed International Telecommunication Union conference in Dubai, raised sharp concerns about the explosion in mobile phone usage. Much of the Dubai coverage had focused on the opposition raised by the United States and allied countries to giving the ITU more control over the Internet. But their success in that opposition, O'Brien said, could well turn out to be pyrrhic.

"In the next decade, a large part of end-user Internet traffic will be shifting to mobile broadband devices," he wrote, noting that those mobile networks are mostly run by the same telecoms that are so influential in the ITU– and regulated by local governments. "Mobile companies are free to block protocols like Skype, censor websites, and spy on their users, with little oversight or global condemnation."

O'Brien concluded: "It would be a tragedy if the pioneers of the Internet fought off the slow-moving bureaucratic threat of the ITU, only to lose control of their ideals to those same forces in the fast-moving and unregulated wilds of the mobile Internet … [T]he real losers would be journalists and their audiences, reading news on a mobile but spied-upon and censored Internet."[71]

Intermediaries: Weak Links in the Chain?

If someone–whether a government or a corporate lawyer–wants to block you from expressing yourself freely online, they may not bother coming after you directly. It may be easier, and quicker, for them to go after one of the "intermediary" companies that stand between you and your users.

That intermediary may be a telecom, but there are plenty of other options to choose from that may be smaller and easier to target. They can include the hosting companies that house the websites of individual users; the Internet Service Providers (ISPs) that provide the connection to the Internet; and the search engines that make it possible to find what you're looking for, among others.

Some may be large corporations, but commonly, they're much smaller, lacking the resources–or the clout, or, perhaps, even the desire–to resist the pressures of censorship.

The Electronic Frontier Foundation has an enlightening report on this topic.[72] It explains:

"Each intermediary is vulnerable to some degree to pressure from those who want to silence the speaker. Even though the Internet is decentralized and distributed, 'weak links' in this chain can operate as choke points to accomplish widespread censorship."

A 2009 report from *China Digital Times*, for example, provided a leaked document from the Chinese Internet search giant Baidu, listing keywords blocked from Baidu searches. A translation accompanying the list includes words such as: *demonstration; AIDS; petition; collective protest; impact on the masses*.[73]

Not all cases of intermediaries blocking content are government ordered, and not all are in repressive countries. For example, Jenna Burrell, an assistant professor in the School of Information at the University of California-Berkeley, points to the potential impact of network administrators, often based in the United States.

Burrell spent years studying the Internet habits of Ghanaian youth. "A less-acknowledged practice of blocking countries on the periphery of the global economy takes place via IP address detection with the intent to prevent users in those locations from accessing certain contents and Web services," she wrote in a book summarizing her research. This is typically done, she said, when network administrators who see a recurring security threat from some region "respond by blocking all traffic from that region."[74]

While Burrell acknowledged in an interview that there may be good reasons for network administrators to be careful based on Internet security or scamming concerns, she hopes for “a conversation that I suspect is not happening about the ideals of open access on the Internet, especially in a global context,” and how network-security actions can affect legitimate users.[75]

A more momentous–and more complicated–case of intermediary as gatekeeper involved the WikiLeaks website, which was hosted on the “cloud” servers of the Amazon subsidiary Amazon Web Services. AWS canceled its hosting arrangement with WikiLeaks in 2011, “immediately following a call from Senator Joe Lieberman for private companies to cut ties with the group,” according to an article in *Forbes* detailing a Harvard law professor’s critique of the Amazon action.[76]

AWS issued a statement saying that it was a violation of the terms of service, not government pressure, that lead them to drop WikiLeaks.[77] But regardless of the motivations, the *Forbes* article concludes that Yochai Benkler’s law-review critique “doesn’t argue that Lieberman’s pressure on Amazon and others to jettison WikiLeaks is illegal. In fact, its legality is exactly what calls into question the future of free speech online.”[78]

Tackling It Head-On: The Global Network Initiative

There are numerous targeted efforts to address problems posed by the issues of maintaining a commitment to free expression and other human-rights principles on the Internet in a world that doesn't universally accept or honor those principles. But there is one effort whose scope and ambition puts it far ahead of any others–even with the caveat that its impact is still not certain.

The Global Network Initiative describes itself as "a multi-stakeholder group [engaged in] a collaborative approach to protect and advance freedom of expression and privacy in the ICT sector."[79]

GNI lists more than 30 member groups, among them ICT behemoths Google, Microsoft, and Yahoo; advocacy groups Human Rights Watch, the Electronic Frontier Foundation, Human Rights in China, and the Committee to Protect Journalists; investor groups Trillium Asset Management and Domini Social Investments; and academic representatives from the Berkman Center at Harvard and the University of California-Berkeley School of Information.

The organization was launched in late 2008, after several years of discussions and negotiations among the different constituencies.

Certainly relevant to those discussions was the publication in 2006 by Human Rights Watch of a lengthy report that sharply criticized various actions of Yahoo, Google, and Microsoft, and called for an end to "the complicity of Western Internet companies in political censorship in China." Human Rights Watch also called for a strong industry code of conduct for the ICT industry.[80]

Two years later, such a code was one of GNI's founding documents: "Principles on Freedom of Expression and Privacy," which draws on a number of international declarations and covenants on human rights. It states, in its preamble, that ICT companies "have the responsibility to respect and protect the freedom of expression and privacy rights of their users." It requires GNI member companies to "implement these Principles wherever they have operational control," and further states that all GNI participants will work both individually and collectively to "engage governments and international institutions" in support of measures to protect freedom of expression and privacy rights.

Finally, and notably, the document has a provision for accountability, stating that initiative participants "will be held accountable through a system of (a) transparency with the public and (b) independent assessment and evaluation of the implementation of these Principles."

It is this element that makes GNI unique, said Susan Morgan, the initiative's current and, so far, only executive director. "As far as I know," she said, "we are the only organization trying to create a standard that has an assessment mechanism built into it … Over time, we'll create a standard for the ICT industry on free expression and privacy rights."[81]

Morgan compared GNI to a similar, earlier process by others in the global economy, including the extractive industries. The question for the companies, she said, is "how can they liquidate the negative impacts and enhance the positive impacts they have on human rights."

The assessments are specified to come in two stages. In the first, an outside assessor evaluates what each company is doing to meet the GNI principles. The second stage adds an outside evaluation of actual incidents in which companies responded "to specific governmental demands implicating freedom of expression or privacy."

Stage one assessments of Google, Microsoft, and Yahoo were done in early 2012; stage two assessments are to be completed later in 2013.

So given a strong set of principles, will the Global Network Initiative actually make a difference?

Maclay, writing in 2010, prior to the completion of the first assessment stage, raised several "criticisms and challenges." Among them, he pointed to what he terms "lackluster participation."[82]

Participation in GNI needs more cultural and geographic diversity, he argued, and a broader range of members, especially ICT companies. He said he was especially disappointed at the absence of telecommunications companies; members of that industry participated in the planning process, he wrote, but then "chose not to continue" when GNI was launched–which "represents an important and missing piece of the puzzle." He would also like to see more of the smaller ICT companies join. "GNI must ask what it needs to do to attract these groups, and also whether their absence has some larger significance," he added.

Still, Maclay, who is on GNI's board of directors, said in an interview that the initiative has had an overall positive effect, particularly considering its relatively small scale and resources. "Even though there were a lot of disagreements there was also a significant level of trust," he said. And he emphasized the challenge of getting large corporations, especially ones that are "highly secretive," and fiercely competitive, to work together and agree to independent assessments that hadn't even been tried before.

"That said, there's lots more that we want to accomplish," he remarked.[83]

Rebecca MacKinnon, a contributor to the 2006 Human Rights Watch report and now a GNI director herself, also is quick to characterize GNI's work as being "still in its early stages." Already, though, its principles "are really kind of becoming an effective standard for what people expect responsible corporate behavior in this area to look like." Those principles, she said, are being cited elsewhere–in Europe, by activist groups, by non-member companies.[84]

"Companies have been doing more thinking through of risks than I saw before" on human rights issues, MacKinnon said. "I've definitely seen changes in company practice that are encouraging," even if the process is not perfect yet.

Google, for its part, sees several values to the initiative. Working with others, for example, "would put us in a better position to say no to outrageous government requests … [and] would also help mitigate against governments playing companies off each other," said Chen, the Google representative. "We believed (and believe) that through collaborative action by a diverse group, we would be able to accomplish more together than alone."[85]

There are numerous targeted efforts to address problems posed by the issues of maintaining a commitment to free expression and other human-rights principles on the Internet in a world that doesn't universally accept or honor those principles.

In its first two annual reports, for 2010 and 2011, GNI noted work by participating companies that aligns with the GNI principles. In the 2010 report, for example, Google cited things it had done that "illustrate how Google implements the GNI Principles to further user privacy and freedom of expression." One of these was the widely praised transparency reports on government and copyright requests that Google launched in 2009.

Yahoo noted its establishment, in 2008, of a dedicated business and human rights program, "to lead its efforts to make responsible decisions in the areas of free expression and privacy." Yahoo's program remains highly visible and active today, with its own dedicated blog that reports on a wide variety of programs including a series of international conferences focusing on women using technology, academic fellowships, and assessments “to understand the human rights implications of our business decisions.”[86]

Microsoft described how it had used the annual ratings from Freedom House, treating all the countries designated as “Not Free” as “High Risk Markets” deserving of special attention when doing business.

It may be impossible to know which of these activities resulted just from the GNI effort. And some of the self-reporting by the companies does seem to show them scrambling to catch up.

In the 2011 annual report, for instance, Microsoft pointed to work it was doing with Human Rights First to face “a challenge in Russia regarding intellectual property rights enforcement actions against the media, NGOs, and other civil society organizations.”

That may all be true–but there was more to the story. The “challenge” involved Russian police raids on anti-government activist groups and the confiscation of their computers, ostensibly to search for pirated Microsoft software. And in fact, lawyers hired by Microsoft had *helped* in those raids, even arguing for criminal prosecution. It was only after the *New York Times* reported this story in 2010 that Microsoft took action.

“After the *New York Times* presented its reporting to senior Microsoft officials, the company responded that it planned to tighten its oversight of its legal affairs in Russia,” according to the article. “Human rights organizations in Russia have been pressing Microsoft to do so for months. The Moscow Helsinki Group sent a letter to Microsoft this year saying that the company was complicit in ‘the persecution of civil society activists.’”[87]

But regardless of how that incident started, the way it ended may demonstrate the value of an organization such as GNI: the outcome was a collaboration between Microsoft and one of GNI’s participating human-rights organizations, creation of a temporary free software licensing program, and moves toward a permanent donation program.

Somewhat less clear is the outcome of stage one of the assessments. All that GNI released, as part of its 2011 annual report, was a very general summary of the “types of recommendations” the independent assessors had issued, with nothing about what recommendations had been issued for which company. In an initiative full of talk about transparency, it seems a remarkably opaque way to share the results.[88]

Board member MacKinnon agreed. “It’s unsatisfactory,” she said about the limited information provided on the assessments. “It’s the issue GNI needs most urgently to address. I expect and hope that the public reporting on the next round will be much more open. It may fly for now, but it’s not going to fly for the long run. The public needs to be better informed.”[89]

Google’s Chen declined to discuss the company’s assessments beyond saying, “We think that the assessments have been useful and fair thus far, but are still a work in progress.”[90] Microsoft and Yahoo did not respond to repeated requests for their comments.

MacKinnon did defend the substance of the assessments–noting, for example, that with all the human-rights and advocacy groups involved as GNI participants, there’s been general approval of the assessments. And indeed, EFF’s Galperin pointed to GNI and its assessment process as one of the positive contributions her own organization was making.[91]

Overall, MacKinnon said, she thinks about GNI’s impact “sort of like how many plane crashes did the good air traffic control system prevent. I don’t know, but it’s probably a lot.”

More Efforts Toward Solutions

Many different players–from members of Congress to free-Internet activists; from people passionate about privacy to those passionate about profits–generally agree that it's important to find a way to stick to the principles of free expression when conducting business in a world that doesn't universally believe in those principles.

Various civil-society organizations–advocacy groups and others–have developed initiatives of their own. Just for example, from three organizations with ties to GNI:

- White papers from the Electronic Frontier Foundation help companies who sell technology to other countries understand when that technology might be used in ways antithetical to human rights. EFF also offers guidance to bloggers, and collaborates in offering software to make certain Web browsers always operate in the encrypted "https" mode that makes Internet use far more secure.[92]
- The OpenNet Initiative, a partnership of three organizations in Canada and the United States, aims to document the "growing global phenomena" of Internet filtering and surveillance and "to promote and inform wider public dialogues about such practices." ONI also offers for download a database file with "ratings of the breadth and depth of Internet censorship in seventy-four countries across four content categories (political, social, Internet tools, and conflict/security)."[93]
- The Center for Democracy and Technology has many initiatives. One recent report, *Shielding the Messengers*, offers practical information about the vulnerability of, and potential protections for, the Internet "intermediaries" that are so often involved, willingly or not, in the repression of free expression online.[94]

Twitter has had its share of criticism for individual actions. But it has also received widespread praise and media attention for its utility in democracy movements around the world and generally gets high marks for how it comports itself when faced with international controversy. Twitter implemented its own transparency reports in July 2012, publishing data starting with January of that year, and acknowledging it had been "inspired by the great work done by our peers @Google."[95]

The major corporations typically have corporate blogs, which promote new services or applications, or share stories of what they did with some recent event, such as the Academy Awards. Several go much further, with blogs and postings that deal with larger issues. Yahoo has particularly focused attention on human rights, giving that topic a blog of its own: http://www.yhumanrightsblog.com/. Yes, the material could be termed self-promotional; still, it gives the company's commitment an open and public space, providing anyone with the markers they can use to rate Yahoo's actions.

And Google, which may hold the record for the sheer number of blogs,[96] operates several with specific applicability to free-expression and privacy concerns–notably, its Public Policy Blog, in which high-level company executives regularly discuss these issues and applications to Google products.[97]

Beyond what the U.S.-based *Tea Leaf Nation* is doing to provide a window on China's microblogs, several Chinese organizations are working to counter the Chinese mechanisms of censorship and control. Notable among them:

- The Chinese Internet censorship-monitoring site Greatfire.org provides regular coverage on the censorship scene through its blog, and it was the first to report that Google had quietly dropped its warning about censored searches in December 2012. They also have an initiative called "Freeweibo" that promises the ability to search for "thousands of keywords that are blocked on Sina Weibo."[98]

- The Journalism and Media Studies Centre at the University of Hong Kong, which runs the China Media Project monitoring the broad range of Chinese media, has also developed "Weiboscope," an up-to-the-minute tool for watching activity on Sina Weibo.[99]

The topic of free expression globally on the Internet hasn't escaped the attention of U.S. lawmakers. In the wake of Yahoo's missteps in China, legislation titled the Global Online Freedom Act was introduced in Congress in 2006 by Rep. Chris Smith, Republican of New Jersey. It would require Internet companies doing business in certain repressive countries designated by the State Department to file annual reports on how they have dealt with human-rights issues. Companies actively participating in GNI would be exempted.[100]

But it's probably fair to say nobody needs to worry about this legislation becoming law anytime soon. First, not even the human-rights community is wholeheartedly behind it.[101] And more to the point, it hasn't exactly sparked a groundswell in Congress. The latest version of the bill was introduced in the House of Representatives and referred to committee in February 2013. Its prognosis of getting out of committee is 2 percent, and its chance of final passage is zero percent, according to a legislative tracking website.[102]

Conclusions

What's happened during the Internet/digitized information revolution is similar to what happens with every big technological advance, Colin Maclay said. After a period of time, "we settled on the norms, and we were generally comfortable with them." Then things change again, "and it's a question of us setting new norms about what's right."

And while stressing that he'd be "incredibly naïve" if he professed to have all the answers in this complex, rapidly changing area, he said he thinks we're making progress. "We have some norms, but not a full set of norms, and maybe we shouldn't be surprised at that. It's not all bad.

"We're in a better place than we were–and a long way from where we need to be."

The ICT companies that have grown from babies to behemoths in the past 20 years, as the primary organizers and managers of the networks that now connect us all, are at the center of the conversation. In a great many respects, their policies and actions are far more mindful of human rights issues than the industrial titans of the past. But free-expression advocates are fair to challenge the companies to act more openly in recognizing the responsibilities that come with their evolving role as gatekeepers of information.

"The debate that needs to happen on the national scale is to ask outright that companies themselves cannot be the final arbiters, which they are by default right now," said Earp of Freedom House. "One of the challenges is how to make sure we don't leave these decisions up to a handful of people in an office somewhere."

None of the experts consulted for this report is particularly enthusiastic about any formal, international form of Internet governance. Everyone from Internet corporations to free-speech advocates turned out in December 2012 to lobby against even a possibility that a U.N.-based organization, the International Telecommunication Union, should have greater power over the Internet.

But neither do they think that no action is required. "The idea that the web cannot be regulated is long gone," said the University of Washington's Karine Nahon. "The question is *who* is going to regulate it?"

She, and others close to the topic, say that dealing with the complexities of the Internet, and the potential collisions between rights issues, commercial practices, and governments, will require collaborative action involving industry members, citizen/advocacy groups, government regulators, and users. "Where you don't get that kind of a broad-based alignment among a number of actors, it seems to be a bit harder," MacKinnon said.

That's not to say that targeted approaches won't help in any such solution. MacKinnon, for instance, said she is working on an effort that would eventually allow thorough, published ratings of ICT companies on their policies and practices, including foreign-based ones. That sort of rating, she said, by "informing people in a systematic way," would help make the sort of broader, collaborative effort she supports more likely.

Danny O'Brien argues that "the problem right now is that the technology has raced ahead of the established norms, even in places like the United States and Europe. Even established democracies don't have the kind of protection we'd like to see," he said, and particularly with respect to mobile technology and privacy rights. He favors concentrating on formulating stronger laws and regulations in the big democracies. "If you create new norms in those countries, and mandate those norms, then the technology is going to reflect those norms" as it spreads around the world.

And then there is the matter of self-regulation.

The big Internet companies may not have fully acknowledged it, but most expert observers agree that these companies have indeed taken on many of the roles of gatekeepers. And those observers also largely agree this demands some greater level of internal transparency.

There is plenty of precedent for this, and particularly from the traditional gatekeepers. One of the most respected of those, the *New York Times*, is widely admired for the depth and the credibility of its reports, and for its commitment to the same sort of high principles companies such as Twitter and Google hold to.

Yet it also is willing to openly acknowledge its fallibility. The *Times* publishes a dozen or so corrections every day, and, more to the point of this discussion, when it has made major gaffes in recent years, it has also made major efforts to mitigate them in the most transparent way possible: in its own pages. After the debacle over plagiarism and fabricated stories by reporter Jayson Blair in 2003, the paper not only published an extraordinary, 7,000-word-plus report on the affair by a team of reporters, it also instituted the post of public editor–an independent contractor who writes in the *Times* on questions of content and standards. That position is still active today.

Media companies do things like this–sometimes under pressure, and sometimes only after missteps–as a way of communicating openly about what amounts to failures of, well, their own "algorithms," the internal systems designed to keep their gatekeeping not only useful to their audience, but in line with their principles.

Tarleton Gillespie suggests ICT companies consider some internal structure that could provide the public with what he calls "transparency of strategy and purpose." This wouldn't have to violate proprietary boundaries. It would also provide, as Gillespie added, "more public accountability on the character of the choices companies make."

Expecting the public simply to trust their avowed commitment to free expression and openness is not enough, in other words. Just consider what happened in the related area of privacy. After long avowing its own commitment to the privacy of users, Google was forced to acknowledge its failings and implement reforms in March 2013. Settling a lawsuit brought by the attorneys general of 38 states over its mapping program, Google agreed to pay a $7 million fine. But far more significant, the company is required to carry out a number of specific internal steps, including extensive annual privacy training for employees and attorneys, and outreach to users about protecting their own privacy.[103]

External regulation of this sort in areas that involve free speech and expression would be more problematic, but no less important to users. The message to Google and its peers should be clear: Acknowledgement of your role in the new world of information is vital, along with a clearly delineated, highly transparent form of internal checks, monitored by an accountability system such as the one GNI is trying to institutionalize.

Recommendations

- **To the ICT companies: Take us inside…honest, and openly.** If she were to have an audience of these corporate executives, Freedom House's Madeline Earp said, the first thing she would tell them would be: "Transparency is your friend." Google and Yahoo in particular have terrific blogs with all sorts of useful information, a lot of it on topics like human rights around the world or documentation of governmental efforts to quash free expression or tips about how to protect anonymity online. And if they see something that could threaten their open-Internet terrain, as they did with the ill-fated Stop Online Piracy Act, they respond ferociously, publicly, and articulately.

  So why is there not even a single blog at a single one of the top companies in which corporate officials can talk frankly with their public to explain the internal conversations and debates that resulted in important content posting or takedown decisions? An ombudsman at a place like Google, or Twitter, or Facebook? "That strikes me as rather a good idea, because of the role they play in mediating these things," Rebecca MacKinnon said. But short of that, even periodic sharing of the internal debates and thought processes would be a valuable first step.

- **To the newcomers: Think about big issues *first***. If we've learned anything in watching the current tech revolution, it is that we shouldn't assume that the companies on top today will be on top tomorrow. Ideas that are not yet even a scrap of code in some college sophomore's brain will be the next big start-ups–and, Colin Maclay hopes, their founding documents won't just be about IPO profits, but also about the higher principles that are still evolving at the established companies. "I hope that the next generation of companies that's forming now has something akin to privacy and transparency in their mission statement," he said, "hard-baking it in the beginning, realizing that they're going to be facing challenges, from governments, from gatekeeping functions."

  Eva Galperin of EFF takes that idea a step further. "What I would really like to see one day, my starry-eyed dream, is that venture capitalists would become more aware of these problems, and require companies, before they invest in them, to go through sort of a boot camp on these issues"–privacy, transparency, and the rest.

- **To Twitter, Facebook, the telecoms, and other ICT companies: Get on board!** MacKinnon, who is as familiar with these issues as anyone, explains why she would "very much" like to see Twitter join the Global Network Initiative. "They are already doing a lot of things that align with GNI principles," she said, "except they are just expecting the public to trust them. And despite their feeling that they can go it alone, over time they're going to realize that it's better to point people to an independent auditing group" than simply to say that they're doing the right thing.

  Twitter should join. Facebook, whose one-year status as a GNI observer was scheduled to end in May 2013 and cannot be renewed, should step up and become a full member. All the industry members, working with the other GNI constituencies, should use their considerable leadership power to help broaden the membership beyond just the big Internet companies– and beyond the borders of the United States. As Earp said: "GNI needs to be making the argument more compellingly to the tech companies that this is something users will welcome, and many countries around the world will welcome."

- **To the Global Network Initiative: Time to toughen up.** Considering the challenging nature of its goals, and the range of highly diverse participants, the work GNI has done in launching itself is highly laudable. But it has been more than three years since its launch, and if the organization means what it says about its long-term mission, it must move at least to require a more transparent process with its assessments of the big corporate participants. MacKinnon is right that it's not enough for Twitter just to say "trust us." That's equally true for GNI. The public needs and deserves more than that.

- **To the users: Pay attention, and weigh in.** This comes in two parts:

  1. Maclay said we should be promoting better "engagement with the tools, in a thoughtful and informed way," helping youngsters understand what is really going on with the new technology and how best to use it. There's a role here for schools, parents, and informal learning centers.

  2. We are too easily lulled by the convenience of our gadgets, as Maclay also notes, and we cannot forget the threats to privacy and free expression this technology can

hold. The public needs to make its voices heard to work against those threats: by supporting the work of groups like EFF, CPJ, or CDT and the various human-rights organizations–and by making its voices heard at the ICT companies in favor of transparency in the same way those companies rally support for their own chosen causes.

Endnotes

1. Madeline Earp, Asia analyst, Freedom on the Net project, Freedom House, telephone interview with author, New York, February 19, 2013.

2. Colin Maclay, managing director, Berkman Center for Internet and Society, Skype interview with author, Cambridge, Massachusetts, February 17, 2013.

3. For several versions of this, see Section 8.12 at this “Libraries FAQ” site: http://www.ibiblio.org/librariesfaq/sect8.htm.

4. Rebecca MacKinnon, “Let’s Take Back the Internet,” video of her talk at the TEDGlobal conference in Edinburgh, Scotland, July 2011, http://www.ted.com/talks/rebecca_mackinnon_let_s_take_back_the_internet.html.

5. Colin Maclay, “Protecting Privacy and Expression Online,” chapter in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace,* Cambridge, Massachusetts, MIT Press, April 2010, http://www.cyberdialogue.ca/wp-content/uploads/2011/03/Colin-Maclay-Protecting-Privacy-and-Expression-Online1.pdf.

6. Tarleton Gillespie, associate professor, Department of Communication, Cornell University, telephone interview, Ithaca, N.Y., February 8, 2013.

7. Quoted in Karine Nahon, “Toward a Theory of Network Gatekeeping,” *Journal of the Am,erican Society for Information Science and Technology,* 59(9), 2008, http://courses.washington.edu/insc555/wordpress/wp-content/readings/Barzilai-Nahon_2008.pdf, p. 1494. (For more on Shoemaker, see: http://shoemaker.syr.edu/.)

8. Christine Chen, senior manager for free expression and international relations, Google, telephone interview with author, Mountain View, California, February 26, 2013.

9. Karine Nahon, associate professor, Information School, University of Washington, Skype interview with author, February 4, 2013.

10. Trevor Timm, “Why the Olympics, NBC Should Embrace Free Speech in Wake of Guy Adams Affair,” MediaShift, PBS.org, August 1, 2012, http://www.pbs.org/mediashift/2012/08/why-the-olympics-nbc-should-embrace-free-speech-in-wake-of-guy-adams-affair214.html.

11. Laura McGann, “Mark Fiore can win a Pulitzer Prize but he can’t get his iPhone cartoon app past Apple’s satire police,” Nieman Journalism Lab, April 15, 2010, http://www.niemanlab.org/2010/04/mark-fiore-can-win-a-pulitzer-prize-but-he-cant-get-his-iphone-cartoon-app-past-apples-satire-police. Also see: Mitch Wagner, “Pulitzer-winning political cartoonist will resubmit banned iPhone app,” Computerworld, April 19, 2010, http://blogs.computerworld.com/15955/iphone_pulitzer.

12. Timothy B. Lee, “As Curiosity touches down on Mars, video is taken down from YouTube,” ArsTechnica, August 6, 2012, http://arstechnica.com/tech-policy/2012/08/as-curiosity-touches-down-on-mars-video-is-taken-down-from-youtube/.

13. Tamas Szigeti, “Why did Facebook delete a call for an anti-fascist rally in Hungary?” FreeSpeechDebate,

December 21, 2012, http://freespeechdebate.com/en/2012/12/why-did-facebook-delete-a-call-for-an-anti-fascist-rally-in-hungary/.

14. Tarleton Gillespie, "The relevance of algorithms," essay from a forthcoming (Fall 2013) book, linked to on Culture Digitally, http://culturedigitally.org/2012/11/the-relevance-of-algorithms/, November 26, 2012.

15. Gillespie, interview with author.

16. The *New York Times* has been experimenting with the comment section on its website, most notably with the coverage of the election of Pope Francis I. The new approach allows readers to filter their own comments by type and to determine what comments they want to read, for example, "positive" or "negative" comments. http://www.niemanlab.org/2013/03/habemus-opinionem-the-new-york-times-experiments-with-more-structured-online-comments/.

17. For example: An index to Twitter's rules and guidelines, https://support.twitter.com/groups/33-report-a-violation; Facebook's "Statement of Rights and Responsibilities," http://www.facebook.com/legal/terms; the terms of service of the Russian social-media site VK, http://vk.com/help?act=cc_terms; the policies of the South African site Mxit, http://site.mxit.com/pages/policies; and YouTube's terms of service, http://www.youtube.com/t/terms.

18. The incident provoked an amusing post on *The New Yorker* magazine's cartoon-department blog: http://www.newyorker.com/online/blogs/cartoonists/2012/09/nipplegate-why-the-new-yorker-cartoon-department-is-about-to-be-banned-from-facebook.html, September 10, 2012.

19. For more complete background: Emil Protalinski, "Facebook clarifies breastfeeding photo policy," ZDNet, http://www.zdnet.com/blog/facebook/facebook-clarifies-breastfeeding-photo-policy/8791, February 7, 2012.

20. "The Twitter Rules," https://support.twitter.com/groups/31-twitter-basics/topics/114-guidelines-best-practices/articles/18311-the-twitter-rules.

21. App Store guidelines, which are otherwise only accessible to registered developers, were published in Leander Kahney, "Here's the full text of Apple's new app store guidelines," Cult of Mac, http://www.cultofmac.com/58590/heres-the-full-text-of-apples-new-app-store-guidelines/, September 9, 2010.

22. Christina Bonnington and Spencer Ackerman, "Apple rejects app that tracks U.S. drone strikes," Wired, http://www.wired.com/dangerroom/2012/08/drone-app/, August 30, 2012.

23. Jay Stanley, "Apple, drone strikes, and the limits of censorship," ACLU, http://www.aclu.org/print/blog/free-speech-national-security-technology-and-liberty/apple-drone-strikes-and-limits-censorship, September 5, 2012.

24. For a good discussion, and collection of links, see: "Netizen Report: Gaza Edition," Global Voices Online, http://advocacy.globalvoicesonline.org/2012/11/22/netizen-report-gaza-edition, November 22, 2012.

25. Matt Buchanan, "The thin red line of terms of service," BuzzFeed, http://www.buzzfeed.com/mattbuchanan/the-thin-red-line-of-terms-of-service, November 15, 2012.

26. Mathew Ingram, "Israel and Twitter: Where does free speech end and violence begin?" GigaOM, http://gigaom.com/2012/11/15/israel-and-twitter-where-does-free-speech-end-and-violence-begin, November 15, 2012.

27. Lee Siegel, "Twitter can't save you," Sunday Book Review, *The New York Times*, http://www.nytimes.com/2011/02/06/books/review/Siegel-t.html?pagewanted=all&_r=0, February 4, 2011. And see: http://www.evgenymorozov.com.

28. Danny O'Brien, then Internet advocacy coordinator, Committee to Protect Journalists, telephone interview with author, San Francisco, February 13, 2013. Since the interview, O'Brien has taken a new job as international director with the Electronic Frontier Foundation.

29. Galperin, interview with author.

30. *Freedom on the Net 2012*, Freedom House, http://www.freedomhouse.org/report/freedom-net/freedom-net-2012.

31. Earp, interview with author.

32. One of numerous examples in "Internet enemies: Iran," Reporters Without Borders, http://en.rsf.org/internet-enemie-iran,39777.html.

33. Jillian York, "Bahrain blocks YouTube pages and more," Global Voice Online, http://advocacy.globalvoicesonline.org/2011/02/14/bahrain-blocks-youtube-pages-and-more, February 14, 2011.

34. "Beset by online surveillance and content filtering, netizens fight on," Reporters Without Borders, http://en.rsf.org/beset-by-online-surveillance-and-12-03-2012,42061.html, March 13, 2012.

35. "Google and Facebook block content in India after court warns of crackdown," *The Guardian*, http://www.guardian.co.uk/world/2012/feb/06/google-facebook-india, February 6, 2012.

36. "Police tensions with Facebook 'inevitable,'" *Sydney Morning Herald*, http://www.smh.com.au/technology/technology-news/police-tensions-with-facebook-inevitable-20130110-2chxa.html, January 10, 2013.

37. Jeffrey Rosen, "Google's Gatekeepers," *The New York Times Magazine*, http://www.nytimes.com/2008/11/30/magazine/30google-t.html?pagewanted=all&_r=0, November 28, 2008.

38. Mark Landler and Brian Stelter, "Washington taps into a potent new force in diplomacy," *The New York Times*, http://www.nytimes.com/2009/06/17/world/middleeast/17media.html?_r=0, June 16, 2009.

39. Samer Mohajer and Ellie Violet Bramley, "Unveiled Syrian Facebook post stirs women's rights debate," BBC, http://www.bbc.co.uk/news/world-middle-east-20315531, November 20, 2012.

40. Claire Cain Miller, "As violence spreads in Arab world, Google blocks access to inflammatory video," The *New York Times*, http://www.nytimes.com/2012/09/14/technology/google-blocks-inflammatory-video-in-egypt-and-libya.html?_r=0, September 13, 2012.

41. MacKinnon, interview with author.

42. Christine Chen, senior manager for free expression and international relations, Google, email to author, March 5, 2013.

43. Google Transparency Report, copyright removals, http://www.google.com/transparencyreport/removals/copyright/.

44. Main page: http://www.google.com/transparencyreport/.

45. Eva Galperin, "It's time for transparency reports to become the new normal," Electronic Frontier Foundation, https://www.eff.org/deeplinks/2013/01/its-time-transparency-reports-become-new-normal, January 29, 2013.

46. http://www.google.com/transparencyreport/removals/government/?metric=compliance.

47. Kevin Rawlinson, "Twitter uses new 'country-withheld content' rule to block neo-Nazi group tweets in German," *The Independent*, http://www.independent.co.uk/life-style/gadgets-and-tech/news/twitter-uses-new-countrywithheld-content-rule-to-block-neonazi-group-tweets-in-germany-8216260.html, October 18, 2012.

48. Marcia Hofmann, Rainey Reitman, and Cindy Cohn, "2012: When the government comes knocking, who has your back", Electronic Frontier Foundation, https://www.eff.org/sites/default/files/who-has-your-back-2012_0_0.pdf, May 31, 2012.

49. Jason Pontin, "Free speech in the era of its technological amplification," MIT Technology Review, http://www.technologyreview.com/featuredstory/511276/free-speech-in-the-era-of-its-technological-amplification/, February 20, 2013.

50. Galperin, interview with author.

51. Peter S. Goodman, "Yahoo says it gave China Internet data," *The Washington Post*, http://www.washingtonpost.com/wp-dyn/content/article/2005/09/10/AR2005091001222.html, September 11, 2005.

52. "Internet Censorship in China," *New York Times*, http://topics.nytimes.com/topics/news/international/countriesandterritories/china/internet_censorship/index.html, updated December 28, 2012.

53. V.V.V., "Mr. Kim, tear down that wall; Mr. Xi, carry on," Analects blog, *The Economist*, http://www.economist.com/blogs/analects/2013/01/google-china, January 11, 2013.

54. O'Brien, interview with author.

55. David Wertime, editor, Tea Leaf Nation, Skype interview with author, February 12, 2013. And for an overview of China's Internet companies, see: Derrick Harris, "A peek inside China's internet giants and their massive scale," GigaOM, http://gigaom.com/2013/01/09/a-peek-inside-chinas-internet-giants-and-their-massive-scale/.

56. Alexa Olesen, "Sina Weibo, China's Twitter, leaders microblog craze," *The Huffington Post*, http://www.huffingtonpost.com/2012/08/02/sina-weibo-chinas-twitter_n_1732300.html, August 2, 2012.

57. Madeline Earp, "What China's Weibo censorship does, and does not, reveal," Committee to Protect Journalists, http://www.cpj.org/blog/2012/06/what-chinas-weibo-censorship-does-and-does-not-rev.php, June 28, 2012. Note the links to individual research reports on the censorship.

58. Earp, interview with author.

59. Analects blog, *The Economist*, op cit.

60. Bill Bishop, "Sina admits it has not complied with weibo real name registration rules," DigiCha (Internet and Digital Media in China), http://digicha.com/index.php/2012/04/sina-admits-it-has-not-complied-with-weibo-

real-name-registration-rules, April 28, 2012.

61. Andrei Soldatov and Irina Borogan, "The Kremlin's new Internet surveillance plan goes live today," Wired, http://www.wired.com/dangerroom/2012/11/russia-surveillance/all, November 1, 2012.

62. Earp, interview with author.

63. Megan Garber, "The age of surgical censorship," *The Atlantic*, http://www.theatlantic.com/technology/archive/2013/01/the-age-of-surgical-censorship/266875/, January 7, 2013.

64. Jennifer Preston, "Syria restores access to Facebook and YouTube," *The New York Times*, http://www.nytimes.com/2011/02/10/world/middleeast/10syria.html, February 9, 2011.

65. O'Brien, interview with author.

66. Maclay, interview with author.

67. Nikhil Pahwa, "Updated: India bans bulk SMS till October 1st 2010; why the ban won't work," Midi4Nama, http://www.medianama.com/2010/10/223-india-bans-bulk-sms-for-3-days-why-the-ban-wont-work/, October 5, 2010.

68. "Some Internet cafes ordered to close," Reporters Without Borders, http://en.rsf.org/cambodge-some-internet-cafes-ordered-to-14-12-2012,43789.html, December 14, 2012.

69. Farnaz Fassihi, "Iran's censors tighten grip," *Wall Street Journal*, http://online.wsj.com/article/SB10001424052702303717304577279381130395906.html, March 16, 2012.

70. *Freedom on the Net 2012*, op cit., page 81.

71. Danny O'Brien, "In Internet freedom fight, why the ITU matters (for now)," http://cpj.org/internet/2012/12/why-the-itu-matters.php, December 18, 2012.

72. "Free speech is only as strong as the weakest link," Electronic Frontier Foundation, https://www.eff.org/free-speech-weak-link#home.

73. "Baidu's internal monitoring and censorship document leaked," *China Digital Times*, http://chinadigitaltimes.net/2009/04/baidus-internal-monitoring-and-censorship-document-leaked, March 3, 2013. Also see: Adam Martin, "Only China may censor Chinese search engines," The *Atlantic Wire*, http://www.theatlanticwire.com/global/2012/08/only-china-may-censor-chinese-search-engines/55452, August 6, 2012.

74. Jenna Burrell, *Invisible Users: Youth in the Internet Cafes of Urban Ghana*, Cambridge, Massachusetts, MIT Press, 2012, page 192.

75. Jenna Burrell, assistant professor, School of Information, University of California, Berkeley, telephone interview with author, Berkeley, California, February 5, 2013.

76. Andy Greenberg, "Harvard Law prof: Amazon's WikiLeaks shutdown set dangerous precedent," *Forbes*, http://www.forbes.com/sites/andygreenberg/2011/02/22/harvard-law-prof-amazons-wikileaks-shutdown-set-dangerous-precedent, February 22, 2011.

77. Undated statement from Amazon Web Services, http://aws.amazon.com/message/65348.

78. For the full article see: Yochai Benkler, “A Free Irresponsible Press: Wikileaks and the battle over the soul of the networked fourth estate,” Harvard Civil Right-Civil Liberties Law Review, http://harvardcrcl.org/wp-content/uploads/2009/06/Benkler.pdf, Vol. 46, 2011.

79. Unless otherwise noted, general information about the Global Network Initiative comes from the organization’s website, www.globalnetworkinitiative.org.

80. *Race to the Bottom: Corporate Complicity in Chinese Internet Censorship,* New York, Human Rights Watch, 2006, http://www.hrw.org/en/reports/2006/08/09/race-bottom.

81. Susan Morgan, executive director, Global Network Initiative, telephone interview with author, Washington, D.C., February 17, 2013.

82. Colin Maclay, “Protecting Privacy and Expression Online,” op cit.

83. Maclay, interview with author.

84. MacKinnon, interview with author.

85. Chen, email to author.

86. “Business and Human Rights at Yahoo,” http://www.yhumanrightsblog.com/.

87. Clifford J. Levy, “Russia uses Microsoft to suppress dissent,” The *New York Times*, http://www.nytimes.com/2010/09/12/world/europe/12raids.html?_r=2&, September 11, 2010. It’s worth nothing that Microsoft did *mention* this article in its section of the 2010 GNI annual report; but it did not acknowledge that the *Times* article helped convince the company to take action.

88. The 2011 annual report can be found at: http://globalnetworkinitiative.org/files/GNI_2011_Annual_Report.pdf.

89. MacKinnon, interview with author.

90. Chen, email to author.

91. Galperin, interview with author.

92. See, Electronic Frontier Foundation: https://www.eff.org/work.

93. See, OpenNet Initiative: http://opennet.net/.

94. “New report and advocacy toolkit on intermediary liability,” Center for Democracy and Technology, https://www.cdt.org/blogs/andrew-mcdiarmid/1312new-report-and-advocacy-toolkit-intermediary-liability, December 13, 2012.

95. “Twitter Transparency Report,” http://blog.twitter.com/2012/07/twitter-transparency-report.html, July 2, 2012. Also see: Christina Farr, “Google praises Twitter for efforts to crack down on Internet censorship,” VentureBeat, http://venturebeat.com/2012/07/02/google-twitter-transparency/, July 2, 2012.

96. For an index of Google’s blogs, see: http://www.google.com/intl/en/press/blog-directory.html#tab0.

97. Google’s Public Policy blog: http://googlepublicpolicy.blogspot.com.

98. For the website's main page, see: https://en.greatfire.org. For particularly useful commentary, see the blog: https://en.greatfire.org/news/blog. Background on Google's decision, and Greatfire.org's reporting of it: Josh Halliday, "Google's dropped anti-censorship warning marks quiet defeat in China," *The Guardian*, http://www.guardian.co.uk/technology/2013/jan/04/google-defeat-china-censorship-battle, January 7, 2013.

99. The China Media Project: http://cmp.hku.hk/about. For a sample "Weiboscope" page, see: http://research.jmsc.hku.hk/social/obs.py/sinaweibo.

100. "Free to choose: Governments and internet firms are wrestling with the rules for free speech online," *The Economist*, http://www.economist.com/node/21564198, October 6, 2012.

101. Rebecca MacKinnon, "Internet freedom starts at home," *Foreign Policy*, http://www.foreignpolicy.com/articles/2012/04/03/The_Worlds_No_1_Threat_to_Internet_Freedom?page=0,1, April 3, 2012.

102. See: "H.R. 491: Global Online Freedom Act of 2013," http://www.govtrack.us/congress/bills/113/hr491.

103. David Streitfeld, "Google concedes that drive-by prying violated privacy," The *New York Times*, http://www.nytimes.com/2013/03/13/technology/google-pays-fine-over-street-view-privacy-breach.html?hpw, March 13, 2013.

Advisory Council
for the
Center for International Media Assistance

Esther Dyson

Stephen Fuzesi, Jr.

William A. Galston

Suzanne Garment

Mark Helmke

Ellen Hume

Jerry Hyman

Alex S. Jones

Shanthi Kalathil

Susan King

Craig LaMay

Caroline Little

Richard Lugar

Eric Newton/
Amy Starlight Lawrence

William Orme

Dale Peskin

Adam Clayton Powell III

Monroe E. Price

Adam Schiff

Kurt Wimmer

Richard Winfield

Center for International Media Assistance
National Endowment for Democracy
1025 F Street, N.W., Suite 800
Washington, DC 20004

Phone: (202) 378-9700
Fax: (202) 378-9407
Email: CIMA@ned.org
URL: http://cima.ned.org

CIMA Center for International Media Assistance

NED National Endowment for Democracy
Supporting freedom around the world