5

Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet

Jonathan Zittrain and John Palfrey

Introduction

Picture a corporate boardroom in the headquarters of a large information technology company in the north of Europe. The chief business development executive has just made a pitch to the board: the company should offer its Internet-based service, delivered over a variety of devices, in east Asia. Her plan is that the firm should start with the white-hot Chinese market and then turn to Vietnam, Thailand, and Singapore. Each of these new markets promises enormous growth.

In each case, the plan calls for a strategy of first entering into joint ventures with local Internet companies, then seeking local investors to set up a stand-alone subsidiary once each trial is successful. Competitors, she argues, will not be far behind. The company might well find itself in the posture of the follower if it does not move quickly. Several board members, each of them outside investors, sound a note of approval.

The general counsel, though, has a few words of warning before the board takes a vote on the proposal. He is concerned about the regulatory requirements that the corporation will face in these new markets. The company needs to be prepared to censor the content it is offering, to disallow users to publish certain information through the service, and to turn over information about the identities of its subscribers upon demand. These are typical requirements when operating almost anywhere—even liberal democracies identify information to be removed, such as that which infringes copyright, or meets some test of obscenity. They require help identifying users at times, and some impose blanket data retention requirements for these purposes.

But in more authoritarian places like China the practices have extra bite. The information the government seeks to censor can relate to civic dialogue and freedom, and the people they seek to identify might be political dissidents or religious practitioners. Often, the requirements to redact or block will be stated or implied only generally without specific requests for individual cases, which means that the company must be prepared to operate in something of a gray zone, trying to divine what the regulators have in mind—and act to censor without explicit orders to do so.

To support his case, the general counsel notes that some of America's most prominent Internet companies have found trouble trying to follow local law against a backdrop of international criticism. Yahoo! has been faulted for turning over information about a journalist that allegedly led to his arrest and imprisonment—for no crime that a court in Yahoo!'s home jurisdiction of California could recognize. Cisco has been attacked for selling the routers and switches that make censorship and surveillance possible. So, too, has Microsoft, for offering a blog service that generates an error rejecting ''profanity'' when a user includes the word *democracy* in the title of a blog. Google has come under fire for offering a search product in China that omits certain search results compared to what its other offerings provide. Side-by-side comparisons of a Google image search for *Tiananmen Square* in http://google.com and http://google.cn starkly show the results of censorship; for anyone who can see both sets of images, the latter lacking any shots of a person staring down a tank in 1989, is forced to consider what it would be like to live under an authoritarian regime. There is no reason why we should be any different, he concludes.

Successful technology companies must now focus on more than simply implementing great ideas that people will pay for. In the earliest days of the Internet, the relevant markets were modest in size and close to home. A local Internet Service Provider once could profit by offering a dialup Internet access service over plain old telephone lines to people who lived near the corporate headquarters. Few of the big players involved were large, publicly traded entities. Revenue projections commonly looked like hockey sticks pointing toward bright blue skies. And, most important for the purposes of this chapter, states left alone the Internet and the companies that built it and its many services. The prevailing orthodoxy was that a regulator that required too much of companies doing business on the Internet would unduly restrict the early growth of online activity, and might find associated high-tech jobs going elsewhere. Few states placed any kind of liability or responsibility on intermediaries for troubles arising from the activities and transactions they facilitated.

More than ten years into the Internet revolution, these are no longer the facts on the ground. The Internet is big business in which entrenched players—and not just what were once called dot-coms—with colossal market capitalizations compete with one another over multi-billion-dollar revenue streams. Their markets span much of the globe. Most important, some states have increasingly forced companies that provide Internet services to do more to regulate activity in the Internet space. This approach applies a new kind of pressure on nearly every corporation whose business involves information and communications technologies (ICTs), especially when the pressure is piecemeal or downright contradictory from one jurisdiction to another, and when the desired regulation contravenes the values of the company's owners or customers. While liberal democracies have so far remained remarkably hands-off as the Internet has matured, the desire of more closed regimes to tap the Internet's economic potential while retaining control of the information space confines the options for these firms.

As this book makes plain, over the past five years there has been a steady rise of Internet filtering practices from a handful of states in 2002 to over three dozen states in 2007. The most extensive of these filtering regimes are found in states in the Middle East and North Africa, Asia and the Pacific, and the Commonwealth of Independent States. The job of online censorship and surveillance is difficult for the state to manage itself, if not altogether impossible.

To carry out these practices, states turn to private firms to provide the tools and services necessary to effect the censorship and surveillance. Most of the high-profile incidents of this type have involved well-known technology companies based in the United States and their efforts to enter the Chinese markets. But this issue is about more than a few companies and about more than one emerging market. Almost any business in the information technologies or telecommunications space might find itself in this position. These private firms include hardware manufacturers, software firms, online service providers, and local access providers, among others.

The shareholders in large technology companies reasonably expect continued growth of market volume or share, and improved profit margins. The pull of markets farther from home is powerful. The shares in these firms are often publicly traded by investors in the state in which they are chartered. In many instances, the social norms and conceptions of civil liberties in the new target market are dissonant with the norms and liberties enjoyed where the senior executives and most powerful shareholders of the corporation live. An everyday act of law enforcement in an authoritarian market looks like a human rights violation to a more liberal one. That act may in fact contravene international human rights standards—and some shareholders, concerned about matters beyond growth and profits, are starting to ask hard questions of corporations about their involvement in such practices.

The ethical problem arises when the corporation is asked to do something at odds with the ethical framework of the corporation's home state. Should a search engine agree to censor its search results as a condition of doing business in a new place? Should an e-mail service provider turn over the names of its subscribers to the government of a foreign state without knowing what the person is said to have done wrong? Should a blog service provider code its application so as to disallow someone from typing a banned term into a subject line?

These questions—prompted by the hard cases that lie between simple acts of law enforcement and clear violations of international norms—are not easily answered through legislation or international treaty. Laws fashioned in this fast-moving environment to lay out what orders corporations must resist in authoritarian states—really, laws about laws—may function as a hopelessly trailing indicator. The firms involved in this quandary should not be seen as a single bloc. They represent a range of levels and types of involvement in censorship and surveillance regimes.

In the context of the cyberlaw literature, these questions ask us to assess ''second-order'' regulation of the cyberenvironment. From a public policy angle, the question is not whether to

impose any control over private actors online, but rather what constraints might be placed on those private actors with respect to the first-order regulation. When states disagree with each other, private actors chartered in one state and operating in the other can become proxies in the fight.

The most efficient and thorough way to address this conundrum is for the corporations themselves to take the lead. The corporations, as an industry, are best placed to work together to resolve this tension by adopting a code of conduct to govern their activities in these increasingly common situations. This approach could, at a minimum, clarify to end-users what they need to know about what companies will and will not do in response to demands from the state. At best, the industry might be able to resist the most excessive first-order demands of the state with a corresponding benefit for civil liberties online. The corporations should call upon the knowledge and goodwill of NGOs, academics, public officials, and others to help frame this code of conduct. The drafters of the code should consider neither the firms nor the markets to be singular in terms of their respective ethical obligations, but rather consider them to be disaggregated. The goal of drafting and putting in place a code should be to establish a meaningful, flexible, and lasting solution to the problem of corporate ethics on a filtered Internet, a solution that may be as much process as substance, creating mechanisms for the resolution of questions as they arise that earn the acquiescence of their first-order regulators, and the respect of their customers and their second-order regulators.

First-Order Regulation of the Online Environment

The initial debate over the regulation of the online environment, as we describe in chapter 2, was whether or not states could regulate online activity. Cyberlibertarians—often derided as cyberutopians—took the provocative view that cyberspace was so different that states could not reach it. That debate is now settled. The answer is that they *can*, more or less in the ways that they have regulated offline activity. Whether or not states *should* regulate the online environment in comparable manner to how they have regulated in the past is a more complicated matter.

We refer here to ''first-order regulation'' of the Internet as this first generation of questions. The large issues covered in Lawrence Lessig's *Code and Other Laws of Cyberspace*, the definitive text in this area, comprise a reliable list.[1] Should the state regulate speech online—whether hate speech, political speech, or otherwise? Should the state step in to protect user privacy? Or listen in on the conversations of citizens in the service of law enforcement? What is the proper role of the state in granting and enforcing intellectual property rights in ideas and expression, or brand and trade secrets, in the online environment? In each instance, virtually every state with a significant population online has exerted some control of this ordinary sort.

The story of this chapter, though, is about whether regulation should come into play in response to this first-order regulation of private actors doing business in other jurisdictions. The

relevant first-order regulation is the extent to which states have required corporations to censor search results, to configure software in such a manner as to block certain expression, to collect and turn over data, and so forth.

Second-Order Regulation of the Online Environment: More State Control, Greater Pressure on Private Parties

As more states place pressure on intermediaries to help control the online space, other states may try to prevent such control, often by imposing their own regulations—a form of second-order regulation of the online environment. This notion of second-order regulation presents a new issue: how to evaluate the regulation that some states place on some firms, based in other jurisdictions, when it comes to activity in the online environment.

This issue has arisen most prominently in the context of the United States Congress inquiring into the activities of several of its most prominent technology firms in the Chinese markets, though as we argue in this chapter, the issue is much broader than such a precise frame would suggest. The first-order regulation is China's requirement that a search engine censor the results that are presented to users in response to a search query, as part of broader practices prohibiting online service providers from disseminating information that may ''jeopardize state security and disrupt social stability.''[2] At issue is not simply whether the first-order regulation is warranted, but rather whether the United States should regulate the activity of the firm chartered in its jurisdiction when it competes in the Chinese markets. In some cases, no first-order regulation has yet been applied, but regulation of the second-order type—of the export control variety—has been proposed.

One reason for focusing on this ethical problem at an early stage of its development is that in a global technology marketplace, such second-order regulatory issues are likely to continue to arise. A mode of responding to these issues in the context of online censorship and surveillance may pay dividends over time as structurally similar quandaries come to the fore.

New Markets, New Modes of Control, New Challenges

As Faris and Villeneuve's review of the data in chapter 1 indicates, Internet filtering occurs primarily in three regions of the world: the Middle East and North Africa, Asia and the Pacific, and the Commonwealth of Independent States. China continues to be the case that garners the most public attention, given the size of its market and the extent to which the state has set in motion the world's most sophisticated filtering regime. But China is far from alone, as more than two dozen states carry out some form of Internet censorship and surveillance online. Further, large, regionally powerful states—China, the Russian Federation, and India, for instance—that provide downstream Internet service to smaller states are poised to pass along their filtering as well.

To add to the complexity of the matter, the mode and extent of censorship and surveillance varies substantially from one state to another as the data in this book make plain. There are several ways for states to filter and monitor. The most direct means is through the use of technology. In its simplest form, the state requires the reprogramming of the routers that lie between the individual end-user and the broader network. The job of the new code is to block certain packets from reaching their destination or simply to learn and record the contents of those packets and who is sending or receiving them. Sometimes it is apparent to the end-users that their requests for certain Web pages have been blocked by the state thanks to special messages substituted for the destinations the users have sought; more often, it is not so apparent. The manner and extent to which censorship takes place online is easier to prove, while surveillance is more elusive.

Online censorship and, potentially, surveillance, is carried out through nontechnical means as well. These controls are sometimes imposed by law: end-users might be prohibited from accessing or publishing certain information that is deemed to undermine public order or other state interests. Such laws are typically very broad, hard to understand, and even harder to follow with any degree of precision. These controls are also imposed most effectively as part of a package of *soft controls*, whereby cultural norms drive censorship or surveillance into the home or local community, often resulting in extensive self-censorship.

Integrated Modes of Online Control: Combining the Technical and the Legal

The most salient form of filtering is direct technical control implemented by legal controls trained on private actors who lie between an end-user and the network at large.[3] The state, unable to carry out filtering effectively on its own, requires private actors to carry out the censorship and surveillance for them. This requirement comes as a formal or informal condition of holding a license to provide Internet-related services in that state.

So, for a large search engine like Google, the mandate from the state may be to ensure that search results provided to citizens of that state do not include links to online content banned in that jurisdiction. In some cases, like insistence by the German and French governments that search results to Nazi propaganda be excised, Google's censorship of search results is controversial only to die-hard civil libertarians, especially when the ways to circumvent such filtering are open secrets. (Germans wishing to search for Nazi propaganda can simply use google.com instead of google.de.) In other cases, like China, where a much broader range of politically and culturally sensitive results are excluded, the public response is one of broader concern.

Likewise, the provider of a blog publishing tool may be prompted to include controls that disallow an individual publisher from including certain words in the title of a blog post. Microsoft found itself in this quandary in 2005. After a successful launch of its MSN Spaces product in the United States market, Microsoft rolled out a Chinese version of the service. MSN

Spaces operated differently in China than it did in the United States, however. If a blogger using the U.S.-branded version of the service decided to type *democracy* into the title of a blog post, there is no problem. In China, that same blogger is presented with an error message: ''You must enter a title for your space. The title must not contain prohibited language, such as profanity. Please type a different title.'' Automated screening of content is also coupled with specific interventions: in 2006, MSN abruptly pulled the blog of a Chinese-based journalist using the pseudonym Michael Anti, apparently at the behest of Chinese authorities.[4] Corporations hosting blogs told ONI researchers in interviews of the persistent fear of being asked to perform one-off censorship tasks of this sort. It is plain that these firms do not relish this job, but fear retribution if they do not comply with the local mandates.

An Internet service provider might be required to keep records of the online activity of all or some of its subscribers, or to monitor who seeks to access certain kinds of content. The provider of a Web-based e-mail service might be required to turn over the e-mail messages of a user identified by the government. Yahoo! has been faced with this dilemma several times. In the United States, Yahoo!'s lawyers routinely respond to law enforcement requests for information about subscribers, pairing an IP address or an e-mail name with other subscriber information. But in China, the stakes are different for the same activity: in at least two instances, Yahoo!'s local affiliate, now Alibaba, has turned over information about users of its e-mail service that allegedly has landed journalists in jail. The crime involved, related apparently to political dissent, would be no crime at all if committed in the state where Yahoo! is chartered.

Though less of a concern to multinational firms, cybercafés can be required to maintain logs of who uses their computers. The cybercafé owner can be called upon to report on the identity of a certain Web surfer who used a given PC during a given time interval. Some are asked to call a special number on the fly if the online activity of a customer sets off certain alarms bells.[5] As Internet connectivity increases, often through broad access at shared terminals, this mode of control continues to become more effective over time.

Two Taxonomies of Private Actors Facing This Quandary

Different technology firms are called upon by states to carry out quite different online censorship and surveillance tasks. In seeking to fashion a policy response, it helps to disaggregate the firms implicated in this matter. Two taxonomies, one more helpful than the other, offer ways to disaggregate these firms and those firms that may soon join them in this awkward position.

The first approach is to consider the nature of the firms' business, which is most useful for determining the firms that might get drawn into an ethical controversy of this sort. We include this taxonomy primarily as it is the orientation that casual observers ordinarily bring to the issue. While useful for the purpose of determining to whom this issue is relevant, this taxonomy is far less helpful in terms of informing what to do about it.

The more useful taxonomy considers the nature and level of involvement of the firms in the online censorship and surveillance regimes. The second taxonomy points the way forward more clearly toward a solution by identifying the various ways in which firms are implicated in these regimes and offering means of distinguishing the different types of ethical obligations they may bear.

Types of Firms

Several types of corporations might find themselves called upon to act as gatekeepers. The first corporations to find themselves involved in the censorship and surveillance controversy were technology hardware providers that sold the switches and routers involved in these regimes. In many parts of the world, Internet security firms sell the services and products used in the censorship and surveillance regimes. More recently, content and online service providers, whose customers are typically end-users, have been implicated. Looking ahead, other telecommunications service providers may well find themselves in a similar position as technologies and forms of digital content converge.

Hardware Providers First, technology hardware manufacturers face scrutiny for their sales of routers, switches, and related services to the regimes that carry out online censorship and surveillance practices. According to the critique of human rights activists, companies like Cisco and Nortel that profit from the sale of the hardware that blocks the flow of packets online or enables states to trap and trace online communications are acting unethically. The problem, the critique goes, is akin to the Oppenheimer problem in the context of nuclear technologies. While nuclear technologies can provide energy efficiently to those who need it, the same means can also power weapons of mass destruction of unprecedented power. The hardware manufacturers respond that the technologies sold to regimes that censor and practice surveillance are precisely the same as those technologies sold to firms and governments in states that do not carry out such regimes. This issue is not new, these firms respond. Dual-use technologies present this issue in an untold number of contexts. And the blame should be placed on those who implement the dual-use technologies in the suspect manner, not on those who produce the ''neutral'' technologies.

Software Providers The second class of firms implicated in this matter includes those corporations that sell the software and services that determine what gets blocked, recorded, or otherwise impeded. Internet security firms—such as Secure Computing, Websense, Fortinet, and others—often serve states, corporations, and other institutions that seek to impede the free flow of packets for one reason or another. A library, for instance, might wish to block underage patrons from accessing pornography online. A similar software package could enable a state to configure a proxy server between a citizen and the wider Internet to block or track certain packets. Many of the states in the Middle East and North Africa that have filtering regimes in place rely upon software packages, and corresponding lists of banned sites,

developed and compiled in the United States. These firms make similar arguments to those of the hardware providers: their technologies and services are dual-use in nature. The tool that can protect a child from seeing a harmful image can also keep a citizenry away from politically or culturally sensitive information online. The human rights critique, the firms argue, should be trained on the regimes that apply the services in a manner that violates laws and norms, not at the service providers who make the tools and update the lists. But the lists of banned sites include some nongovernmental organizations that observers suggest have no place there, if in fact, for instance, the notion is just to protect children.

Online Service Providers Most recently, the providers of Internet-based applications have found themselves facing hard questions about their activities in such regimes. A wide range of firms fall in this category: ISPs, e-mail service providers, blog-hosting firms, search engines, and others. ISPs are asked to route traffic in certain ways to prevent citizens from accessing or publishing certain content; likewise, ISP data retention policies are a hot topic of debate in many jurisdictions, as the personal data they keep about citizens is at once sensitive and potentially useful in the context of law enforcement activities. E-mail service providers, such as Yahoo!'s local partner in the Chinese context, are routinely asked to turn over information related to subscribers. The makers of Weblog software and hosting services, such as Microsoft's MSN unit, are asked to block certain information from being published and told to take down the postings or entire blogs of subscribers. Search engines, including Google, are required to limit the results that appear in response to certain queries entered by citizens. The nature of the ethical questions each of these types of firms face varies with the nature of the service they provide and the type of participation the state asks of them. In most instances, corporations respond that they have an obligation to obey local law with respect to services they offer in all jurisdictions.

Corporations often perceive that they do not have the option of resisting the demands of law enforcement officials, for fear that the corporation or their local employees will face sanctions or that their license to operate will be revoked. Some corporations, recognizing the risks inherent in doing business in certain regimes, have limited the types of services that they offer in those contexts to avoid being placed in an uncomfortable role. Google, for instance, decided not to introduce its popular blogging and e-mail tools in the Chinese markets to avoid the possibility of being forced to turn over much information about subscribers, other than possibly basic search query data. In an ironic twist, in Iran, Google has been accused locally of ''censorship'' for failing to bring all of its services into the Iranian market.

Online Publishers Corporations that publish information online are also caught up in this issue, though their situation is somewhat more straightforward. As a general matter, online publishers are treated as other publishers in the states in which they operate, so the ordinary media restrictions that attach to newspapers and other traditional media also attach in the online space. The notion of providing a single news or information service from one place in the

world that is accessible at any other place, so long as it is not censored, remains a viable model. Large media companies, such as the BBC or CNN, tend to adopt this posture. The BBC pays a price for this approach: everything it publishes is blocked in China. When their content is filtered at the destination by the state, they are not complicit.[6] The ethical issue arises only for those firms with local offices and offerings specifically targeting a state that censors online material.

Telecommunications and Other Content Delivery Providers Additional classes of corporations soon could be recruited as gatekeepers. For instance, as mobile telecommunications providers continue to thrive and begin to function as digital content providers, it is only a matter of time before these intermediaries will be pressed into service by states as a requirement of their licenses to operate. Providers of Voice-over Internet Protocol services have already found that their services are sometimes blocked, as in United Arab Emirates. Filtering and surveillance, though posing new technical challenges, may follow. Firms that serve other businesses in delivering online content—including rich media, such as streaming audio and video, in addition to traditional Web pages—also may be subject to such restrictions. Any large-scale intermediary that plays a role in delivering digital information to an end-user might find itself an arm of the state in the online environment—and will have to answer to the same questions as their peers in the hardware, software, and Internet services industries.

Types of Involvement

Another way to categorize the firms that face increasingly difficult ethical questions in this context is to assess not the type of firm, but the type of involvement that a given firm has in the censorship or surveillance regime in question. Though the first taxonomy is simpler, this second taxonomy draws the ethical questions into greater relief. This second taxonomy provides a basis for the different types of ethical obligations that might apply to various firms.

Direct Sales to States of Software or Services to Filter Online Content This category includes those firms that seek to profit from the sale of software or online services, including constantly updated block lists, that states use to implement their online censorship regime. Since these services typically require updates related to the lists used for blocking and since the revenues track directly to the censorship service itself, these firms are the most intertwined with online censorship. An important further distinction emerges between those firms that provide software and those that provide software plus the service of an updated list of sites to block.

Direct Sales to States of Software or Services for Surveillance This category includes those firms that seek to profit from the sale of software or online services, including suites of Internet security systems, that states use to implement their online surveillance regime.

Direct Sales of Dual-use Technology Used in Filtering Online Content This category includes those firms that seek to profit from the sale of Internet-related hardware, including related software and services, that states use to implement their online censorship regime.

Direct Sales of Dual-use Technology Used in Online Surveillance This category includes those firms that seek to profit from the sale of Internet-related hardware, including related software and services, that states use to implement their online surveillance regime. Often, this hardware is sold with related software and services, such as training and support. The more the hardware provider is aware of the usage of the equipment and the more the revenues from services are recurring (rather than a one-time sale of hardware), the more complex the ethical posture the company faces.

Offering a Service that Is Subject to Censorship This category includes those firms that seek to profit from the provision of online services that result in a citizen of a state accessing information in a manner that is censored, such as through a search engine with results omitted or an ISP that refuses access to certain parts of the Internet.

Offering a Service that Censors Publication This category includes those firms that seek to profit from the provision of online services that disallow a citizen of a state from publishing certain information online or that takes down published information at the behest of a state.

Offering a Service with Personally Identifiable Information, Subject to Surveillance This category includes those firms that seek to profit from the provision of online services that capture personally identifiable information about a citizen of a state and where that information may be monitored, searched, or turned over to state authorities upon request.

In certain contexts, the executives of a firm in any of these categories might argue that they do not face a hard ethical question. For instance, in the case of an e-mail service provider that turns over information to a law enforcement officer about a subscriber in a manner that prevents commission of a crime—or, in the most extreme example, an act of terrorism—the corporation may not only have no qualms about its actions, but in fact be proud of its role. By contrast, when the information sought by the state is related to a political dissident whose every action is lawful, or protected by international norms, the ethical landscape is transformed. The same is true with respect to censorship: the blocking or taking down of hate speech, in the context of Germany and France, may well be viewed differently than the blocking or taking down of the expression of certain religious beliefs, for instance. The ethical question in any given instance may ultimately turn less on the precise role of the corporation in the digital ecosystem and more on the nature of the information or the manner in which it is requested of the corporation.

Potential Responses

Reasonable people disagree as to the best means of resolving these emerging ethical concerns. One might thus contend that there is no ethical problem here—or, at least, that the ethical problem is nothing new. If an Internet censorship and surveillance regime is entirely legitimate from the perspective of international law and norms, the argument goes, then a private party required to participate in that regime has a fairly easy choice. If the executives of our hypothetical corporation based in Europe disagree on a personal level with a censorship and surveillance regime, then they should simply exercise their business judgment and refuse to compete in those markets. Alternatively, those executives could decide to refuse to comply with the demands that they believe put their firm in a position in which their ethics are compromised—and then accept the consequences, including possibly being forced to leave the market, that befall them as a consequence of their resistance.

One option from a public policy angle, then, is to do nothing—to accept the status quo, and to let the trend play itself out. In the unlikely event that online censorship and surveillance were to cease across the globe, or if states were to stop calling upon private actors to get the job done, or if corporations were to stop expanding into other markets, the problem might be most cleanly resolved. But absent such changes in the facts as they stand, the stakeholders in these issues have a series of possible ways to move forward to resolve the conflicts.

Industry Self-Regulation

The most likely—and most desirable—means of resolving this problem in the near-term would be for the relevant corporations themselves to come up with a sustainable manner of ensuring that they operate ethically in these charged contexts. It is surprising that no major firm has gone public with such an ethical code before entering a market, such as China, where such problems are sure to present themselves. With firms now competing in those markets, the need to do so is no less acute, whether or not legislative or other action follows.

In the simplest form, individual firms could each develop their own principles, much like a privacy policy on today's Internet; statements could clarify to users, shareholders, and others how the firm will handle these situations. Microsoft set forth a partial version of such a policy at a speech by General Counsel Brad Smith in 2005, in which he pledged the company to follow a ''broad policy framework'' for responding to restrictions on the posting of blog content.[7] The policy included three specific commitments:

> Explicit standards for protecting content access: Microsoft will remove access to blog content only when it receives a legally binding notice from the government indicating that the material violates local laws, or if the content violates MSN's terms of use.
>
> Maintaining global access: Microsoft will remove access to content only in the country issuing the order. When blog content is blocked due to restrictions based on local laws, the rest of the world will continue to have access. This is a new capability Microsoft is implementing in the MSN Spaces infrastructure.

> Transparent user notification: When local laws require the company to block access to certain content, Microsoft will ensure that users know why that content was blocked, by notifying them that access has been limited due to a government restriction.[8]

Microsoft's step to set forth these three commitments is laudable. And despite putting in place these commitments, which sets the firm apart from most competitors, Microsoft's executives have continued to exercise leadership in the industry in the effort to come up with a common set of principles.

But as a policy matter, a firm-by-firm model of this sort, though potentially an expeditious way forward, would suffer from the variation among approaches bound to ensue. Users would be forced to sort through legalese, much as privacy policies and terms of use force the curious to do on today's Internet, and to compare policies of the relevant firms—a task few people are prepared to invest the time to undertake, and which would disadvantage those who cannot easily parse fine print. And by not standing together, the firms would only have as much leverage as each firm has to begin with.

The more promising route would be for one or more groups of industry members to come up with a common, voluntary code of conduct that would govern the activities of individual firms in regimes that carry out online censorship and surveillance. Such a process is underway, coordinated by the Center for Democracy and Technology and by Business for Social Responsibility. Google, Microsoft, Vodafone, and Yahoo! are actively working together on a code. This process profitably includes additional nonstate actors such as NGOs and academics, including the Berkman Center for Internet & Society at Harvard Law School and the University of St. Gallen in Switzerland. Regulators with relevant expertise and authority have been actively involved in the drafting process. The code is intended to set out common principles with enough detail to inform users about what to expect, but without being so prescribed as to make the code impossible to implement from firm to firm and from state to state. The code might also provide a roadmap for when a firm might refuse to engage in regimes that put them in a position where they cannot comply with both the code and with local laws.

If the industry itself does not succeed through such an approach, the likelihood increases that an outside group will come up with a set of principles that will gain traction and place pressure on the companies to act. The Paris-based Reporters Sans Frontières have drafted such a set of principles, as have a group of academics with their base at the University of California, Berkeley. An outsider's code might be something to which firms could be encouraged to subscribe, on the model of the Sullivan Principles and the Apartheid-era South Africa. An institution might emerge to support the principles and the companies that subscribe to them.

Whether drafted by industry members, outsiders, or a combination thereof, the elements of such a code might either be general in nature—a set of core commitments such as transparency, rule of law, the rights of free expression and individual privacy, and so forth—or more specific, according to a taxonomy of the second sort described earlier. The more specific the

code, the more useful, almost certainly, though the reality of getting competing businesses to agree to detailed business practices of this sort is daunting.

As a substantive matter, the code might address censorship and surveillance together, or might disaggregate these topics. Sales to governments of technologies that enable censorship and surveillance presents yet another set of problems that might be taken up in such a code.

By way of example, the framework for such principles on censorship and surveillance might take the following form:

Censorship: Commitment and Guiding Principles At the core of the censorship framework is a company's commitment to the right to free expression. Specific elements of such a commitment might include the following:

1. Formalization. A commitment to establish and carry out formal internal processes for responding to all requests for censorship, whereby the company will respond to requests to censor online information only when presented with formal, written requests from state officials at the appropriate level of authority to make such a demand.

2. Limitation of Scope. Where one state requires that certain online content must be censored, a company will make its best efforts to publish that content in all other markets that the company serves where the content is permitted to be accessed or published online.

3. Reduction of Collateral Censorship. A commitment to make an active effort to uncover instances in which online content that is censored does not fit local legal definitions of what is meant to be censored. A company will work with local authorities to remove from lists of sites to be censored, or otherwise ensure that customers and employees can access, inadvertently blocked online sites or information. A company will maintain a policy for processing complaints about overcensored sites and will take action where complaints are determined to be meritorious.

4. Awareness. The net result of a company's activities in a given country is greater awareness of censorship and filtering by users and lawmakers than if the company were not offering its services in that country. A company seeks to indicate when information that otherwise would have been available is not made available to a user. When one of the company's users is a source of information censored online, the company will seek to inform that user that information they published has been censored. The company will publish, or work with others to publish, information about how censorship works in practice in countries where the company does business and will share data with researchers who study these matters. The company is also committed to supporting the efforts of the international community to uphold universal human rights.

State Demands for User Information: Commitment and Guiding Principles At the core of the framework related to state demands for user information is a company's commitment to the rights of its users to privacy. Specific elements of such a commitment might include the following:

1. Protection from Forced Disclosure. A commitment to establish and uphold rigorous procedural protections to ensure that the company only discloses user information to foreign governments when absolutely necessary under local law.
2. User Notification and Education. A commitment to providing general information about the risks to the company's users of using the company's services on a worldwide basis, as well as specific information about the risks of specific activities in certain settings where those risks are particularly high.
3. Consciousness of Data Location. A commitment to locating servers in places that are unlikely to result in the unethical, forced disclosure of user information. Server location will be based, where possible, in countries with a demonstrated commitment to due process of law and to reliable and consistent rule by legitimate governments. A company will disclose to users the location of its servers hosting their personally identifiable information where possible.

A critical part of such a voluntary code, regardless of its substantive terms, would be to develop an institution that would be charged with monitoring adherence to the code and enforcing violations. One way to accomplish this goal would be for states to adopt the code as law, by passing ordinary legislation and then bringing to bear the full law enforcement capabilities of the state to back it up. Another way could be to imagine an institution—perhaps not a new institution, but a pre-existing entity charged with this duty—that would include among its participants representatives of NGOs or other stakeholders without a direct financial stake in the outcome of the proceedings. This institution may or may not have state regulators involved as partners to ensure compliance. The institution would play an essential role in ensuring that the voluntary code of conduct not only has force over time, but also that it continues to address the ethical issues as they change.

The development of the code itself solves only a small part of the problem; it is in the successful application of the code that a long-term solution lies. In the context of other instances of corporate codes of ethics implicating human rights, such as the sweatshops issue, getting to the code was the easy part.

Law

The legal system might provide one or more ways to resolve the ethical dilemmas facing corporations in the context of states that censor or carry out surveillance online. That said, classic state-based regulation—of the second-order variety—is unlikely to be the most effective means of addressing this particular problem over time. Individual states might require corporations chartered in their jurisdiction to refrain from certain activities when operating in other states.

The analogy in the United States context runs to the Foreign Corrupt Practices Act, which disallows corporations chartered in the United States from bribing foreign officials and other business dealings that would violate U.S. law if carried out in the home market. A ''hands-tying'' regulation of this sort might be combined with other approaches—including the voluntary

code, whether or not embodied in formal law—that might attack parts of the problem, but would unlikely resolve the conflict outright. Such approaches might include funding for pro-democracy activities in the online context, banning the sale of certain technologies, banning the location of servers in certain places, or applying pressure in the context of trade negotiations on those states that are placing the corporations in the hard position.

A member of the United States Congress, Rep. Chris Smith of New Jersey, introduced the Global Online Freedom Act (GOFA) in 2006[9] and again in 2007.[10] This proposed legislation would establish ''minimum corporate standards for online freedom'' and would impose export controls on the sales of any item ''to an end user in an Internet-restricting country for the purpose, in whole or in part, of facilitating Internet censorship.'' The legislation's intent is laudable: to limit the extent to which United States–based corporations participate in censorship and surveillance in other states.

The shortcomings of GOFA point to the difficulty of enacting second-order regulation on this topic at this moment in history. Some of the provisions, such as the requirement that no servers are to be located within the borders of a state deemed to be ''a designated Internet-restricting country,'' might well achieve the statute's aims by simply disallowing most companies from competing in the foreign market in question; providing a service from abroad will often be too slow or too limited by state-level firewalls or filtering to provide a compelling service to the targeted customers, as Google learned in China.[11]

GOFA would also require a United States–based corporation to check with the State Department before providing ''to any foreign official of an Internet-restricting country information that personally identifies a particular user of such content hosting service.'' When combined with a private right of action for any citizen aggrieved by a violation of that section, these provisions are likely to be such an administrative burden on both private and public parties as to be unworkable. The export controls are impossible to evaluate on the merits, since the legislation simply calls upon the secretary of state and the secretary of commerce to work out regulations within ninety days of enactment of the Act. Given the fact that no specifics are provided on the export controls in the proposed Act after months of formal and informal hearings, drafting, and discussion, one is led to believe that coming up with such regulations in ninety days will be a substantial challenge.

Another reason not to rely upon traditional legal mechanisms in this context is that a globally coordinated set of standards will almost certainly take so long to put in place that the contours of the problem will have changed beyond recognition by the time of enactment. Changes to the relevant statutes or treaty may be equally hard-won. The challenge of coordinating adjustments over time across multiple regimes would be enormous. Laws fashioned in this fast-moving environment will function as a hopelessly trailing indicator, especially if an industry-led process does not precede the legislative approach to the problem. The GOFA drafting experience in the United States suggests that law should be seen as a component of a solution, and perhaps the way to memorialize what the relevant industry members adopt, but not the initial approach.

One possibility for a viable long-term solution would be for the industry consensus to be given the status of law over time. This approach would help to address three of the primary shortcomings of the industry self-regulation model. First, self-regulation can amount to the fox guarding the chicken coop. Second, self-regulation permits some actors to opt out of the system and to gain an unfair competitive advantage as a result. Last, the self-regulatory system could collapse or be amended, for the worse, at any time—and may or may not persist in an optimal form, even if such an optimal form could be reached initially.

This mode of ratifying an industry self-regulatory scheme has instructive antecedents. Most immediately relevant, the Sullivan Principles—proposed initially by one man—eventually became incorporated into U.S. law: the Anti-Apartheid Act in 1986 that embodied the Sullivan Principles passed over President Reagan's veto.[12] In the technology context, a series of proposed laws in the United States—some more advisable as public policy than others—have had a similar history. In the case of the Security Systems Standards and Certification Act of 2001 (SSSCA), the Consumer Broadband and Digital Television Promotion Act of 2002 (CBPTPA), and the Audio Home Recording Act of 1992 (AHRA), the industry came to consensus as to a feasible solution to a common problem, which the Congress then took up as possible legislation. The analogy here is not to the merits of each proposal, each of which suffered from deep flaws. The analogy runs instead to the process of the industry working through the details of a common problem, with lawmakers coming along thereafter to ratify the agreement.

The advantages of such a process are several. This approach would lead to a more stable regulatory regime, bringing with it the benefits of administrative, enforcement, and appellate mechanisms. Depending on what emerges from the process, the Congress or their colleagues in other jurisdictions could decline to ratify the agreement if the industry had not moved the bar high enough. This approach would also solve possibly the toughest problem of industry self-regulations, whereby industry outliers who do not opt in may enjoy an unfair advantage, especially in a context like this one where the behavior is hard to codify as good or bad. The function of ratifying the industry-led agreement ex post facto would be to level the playing field for all relevant firms. Local firms might retain their advantage—they would have only the first-order regulation to contend with, not the second-order—but that is another problem of globalization altogether.

International Governance

Problems in cyberspace rarely have been solved through coordinated international action, though there is no inherent reason to believe that international cooperation or governance could not play a meaningful role in resolving these ethical dilemmas. The United Nations has not been involved in extensive regulation of the online space. The primary U.N.-related entity to play a regulatory role in anything related to the Internet is the International Telecommunication Union (ITU), which has a long history in the coordination between states and private

parties in the telecommunications sector. The ITU's role has included the coordination of country codes to facilitate international telephone dialing, which parallels the port allocation process in Internet governance generally handled by the nonprofit Internet Corporation for Assigned Names and Numbers (ICANN). Put in the ITU's own expansive terms, its role ranges ''from setting standards that facilitate seamless interworking of equipment and systems on a global basis to adopting operational procedures for the vast and growing array of wireless services and designing programmes to improve telecommunication infrastructure in the developing world.''[13] But these activities have generally focused on interoperability within the telecommunications sector broadly, and have not extended far into the Internet governance realm.

Other than the ITU, the U.N.'s work relevant to this problem has been handled through the Internet Governance Forum (IGF), chaired by Nitin Desai and under the secretariat of Markus Kummer. The IGF has the authority to conduct an international dialogue on issues related to the Information Society, which has provided a forum for broaching issues but is neither chartered, nor likely, to accomplish any degree of change. An international treaty process, though cumbersome, could emerge as the way ahead. Some activists have considered litigation under existing human rights agreements. More likely than a treaty process, though, the IGF could be called upon to raise this issue squarely with the global community to determine the most promising course of action. Unlike the analogous Sullivan Principles process, though, the technical aspects of the Internet filtering and surveillance issue make it unlikely that a true global community conversation would ensue. Rundle and Birdling have taken up related issues in much greater detail in chapter 4 of this volume.

Other Modes of Pressure

Human rights activists, academics, and shareholder advocates have played an important role to date in the public discourse related to this issue. The United States Congress has held hearings on this matter to draw attention to the actions of large technology firms. The New York City Comptroller has recently filed shareholder actions with certain technology firms to prompt action on these topics. Human rights organizations and investor groups around the world have hosted forums related to corporate involvement in such regimes. While the involvement of NGOs and other outsiders in the process of addressing these ethical issues is not a solution in itself, it is clear that these stakeholders play an important role in any next steps.

Conclusion

The most promising approach to addressing the ethical dilemma facing multinational corporations doing business in states that carry out online censorship and surveillance is for the relevant community to develop a voluntary code of conduct, with the possibility that such a code be redacted into formal law at some later stage. The code can emphasize procedural safe-

guards so that Internet users will know the extent to which their communications have been restricted, altered, or censored due to the contributions of a signatory. The code can bind firms to act only where required, and only where the demands placed upon it are specific and formal. That code must be coupled with the establishment of a reliable mechanism for monitoring and compliance assurance. This approach could, at once, be responsive to the nuanced issues involved, flexible over time as the technologies and politics shift, and sustainable over the long-term. Such a process ought to include at the table the NGO community in a supportive, nonadversarial, mode. State regulators might also be drawn into the process in constructive ways. The affected industry need not—and ought not—go it alone.

Though the environment is too complex and unstable for the standard modes of lawmaking to work in the near-term, states do have a role to play in helping to resolve this tension. A patchwork of competing state laws that restrict corporations chartered in one locale in how they do business in this regard could be counterproductive in others. The challenges inherent in framing the Global Online Freedom Act of 2006 and 2007, in the United States context, point to some of the many hazards of this approach.

The proper role of the state in the context of addressing this problem is twofold. First, those states that are more concerned with what their corporations are doing elsewhere should support and encourage the corporations as they seek to work together to raise the bar for themselves and their competitors. That support might come in the form of involvement and encouragement as the industry works with the NGO and academic communities to derive a set of ethical guidelines. Support might also mean using leverage in trade negotiations to lessen the extent that corporations are placed in this position in the first place—in other words, true state-to-state battles against first-order regulation so that second-order regulation is not necessary. Where constructive, states might consider rule-making that ties the hands of their corporations to provide support for their refusal to operate outside of the bounds of these ethical constraints. But states are unlikely to be able to lead constructively and quickly enough to address this problem alone. States may in fact play their role best as ''fast-followers'' to ensure that the industry-led process results in meaningful and effective second-order regulation of corporate action in these contexts.

On a fundamental level, the states that are increasing Internet filtering and surveillance themselves are best positioned to resolve this tension. In some instances, the primary driver for change might be a careful review of the human rights obligations, whether through treaty or otherwise, that place limits on state sovereignty to act in this manner. Human rights activists may prompt this review through litigation if states do not undertake it themselves. In other instances, the driver might be economic; there is little argument that the development of a competitive environment for businesses using ICTs is a positive factor in economic growth, particularly of developing economies. In either event, states that place restrictions on Internet usage and seek to leverage network usage for purposes of surveillance outside the bounds of human rights guarantees do so at some political and economic peril.

Multinational corporations have every incentive to work hard toward an industry-led, collaborative approach to resolving the tension, regardless of how states act. An industry-led approach could have, at a minimum, the benefit of improved clarity. If the code is well-drafted and well-implemented, users of Internet-based services would know what to expect in terms of what their service provider would do when faced with a censorship or surveillance demand. The benefit of such an approach could well extend further. By working together on a common code, and harnessing the support of their home states, the NGO community, investors, academics, and others, the ICT industry might well be able to present a united front that would enable individual firms to resist excessive state demands without having to leave the market as a result of noncompliance. The ICT industry should strive to provide the best possible services without compromising civil liberties, the generativity of the network, and its democratizing potential.

Notes

1. Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999, 2006).
2. See Internet Society of China, ''Public Pledge of Self-Regulation and Professional Ethics for China Internet Industry,'' http://www.isc.org.cn/20020417/ca102762.htm.
3. See Joel R. Reidenberg, *States and Internet Enforcement*, 1 U. OTTAWA L. & TECH. J. 213 (2003–04); see also John Palfrey and Robert Rogoyski, ''The Move to the Middle: The Enduring Threat of 'Harmful' Speech to Network Neutrality,'' 21 *Washington University Journal of Law and Policy* 31 (2006).
4. Robert Scoble, Scobleizer, http://scobleizer.com/2006/01/03/microsoft-takes-down-chinese-blogger-my-opinions-on-that/ (accessed January 3, 2007) (for a prominent Microsoft employee's discussion of his company's takedown of the Michael Anti blog). See also Rebecca MacKinnon's contemporaneous account, http://rconversation.blogs.com/rconversation/2006/01/microsoft_takes.html (accessed January 3, 2007).
5. Confirmed in multiple interviews by ONI researchers with representatives of U.S. companies doing business in China.
6. See Jonathan Zittrain, ''Internet Points of Control,'' 43 B.C. L. Rev 653 (2003) for a taxonomy of Internet points of control, including conceptions of source and destination filtering.
7. Microsoft Press Pass—Information for Journalists, ''Microsoft Outlines Policy Framework for Dealing with Government Restrictions on Blog Content,'' January 31, 2006, http://www.microsoft.com/presspass/press/2006/jan06/01-31BloggingPR.mspx (accessed January 4, 2007).
8. Ibid.
9. ''H.R. 4780 [109th]: Global Online Freedom Act of 2006,'' GovTrack.us, http://www.govtrack.us/congress/billtext.xpd?bill=h109-4780 (accessed January 3, 2007).
10. ''Smith Reintroduces the Global Online Freedom Act,'' PR Newswire, http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/01-08-2007/0004502076&EDATE= (accessed February 15, 2007).
11. Andrew McLaughlin, ''Google in China,'' the Official Google Blog, http://googleblog.blogspot.com/2006/01/google-in-china.html (accessed January 3, 2007).
12. Winston P. Nagan, ''An Appraisal of the Comprehensive Anti-Apartheid Act of 1986,'' *Journal of Law and Religion*, vol. 5, no. 2 (1987): 327–365.
13. ''Role and Work of the Union,'' International Telecommunication Union, http://www.itu.int/aboutitu/overview/role-work.html (accessed January 3, 2007).