CHAPTER 1.5

Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet

JOHN G. PALFREY, JR., Berkman Center for Internet & Society, Harvard Law School

It is getting harder to be a successful technology company. In the earliest days of the Internet, the relevant markets were modest in size and close to home. A local Internet service provider, for instance, once could profit by offering a dial-up Internet access service over plain old telephone lines to people who lived close by to 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 throughout the world left alone both the Internet and the companies that plied it for profit. The prevailing orthodoxy was that a state that required too much of companies doing business on the Internet would be making a dire mistake by restricting the early growth of online activity. Few states placed any kind of liability or responsibility on intermediaries. Many states even made the Internet a tax-free haven to promote its growth.

Now that we are more than 10 years into the Internet revolution, these are no longer the key facts on the ground. The Internet is big business in which large, entrenched players—and not just what were once called dot-coms—with colossal market capitalizations compete with one another over multibillion-dollar revenue streams. The relevant markets that they reach span much of the globe. But the most important fact that has changed: states have increasingly begun to force 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 communication technologies (ICT).

Internet filtering and surveillance put this phenomenon into stark relief. *Internet filtering* refers to the practice by which states restrict citizens from accessing or publishing certain information on the Internet. Closely related, *Internet surveillance* refers to the means by which states record, listen in on, or track down conversations that take place over the Internet. Over the past five years, the OpenNet Initiative (ONI)—a collaboration that joins researchers at the University of Toronto, the University of Cambridge, the University of Oxford, and Harvard Law School—has tracked the steady rise of Internet filtering practices from only a handful of states in 2002 to more than two dozen in 2007. The most extensive of these filtering regimes are found in states in three regions of the world: the Middle East and North Africa; Asia and the Pacific; and Central Europe and Asia. In the context of this *Report* on the promotion of networked readiness, it is worth noting that this trend cuts directly against the general guidance by Internet development experts in favor of deregulation of the ICT environment in the interest of growth.

The states that employ these filtering and surveillance regimes cannot do the work alone. This simple fact sets up the ethical quandary at the heart of this chapter. Virtually none of the two dozen or so states that filter the Internet have a network controlled entirely by the state. The most successful strategies for accomplishing state-mandated filtering and surveillance, like the Internet itself, are highly distributed in architectural terms. In almost every case, states have to rely upon private actors to carry out most of the censorship and surveillance. The means by which states call upon private actors, and for what purpose, vary from state to state. But the trend points toward greater expectations placed by states on private actors to help get the online censorship and surveillance job done.

For global technology companies, this scenario sets up a hard problem. The shareholders in large technology companies reasonably expect continued growth of market share, improved margins, and so forth. The shares in these firms are often publicly traded by investors in the state in which they are chartered. The pull of markets further from home is obvious and powerful. 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. Sometimes, 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.

Corporations are increasingly finding themselves caught in the crosshairs as they are asked by local authorities to carry out censorship and surveillance online. This chapter describes this growing, thorny problem and some possible means to resolve it. The most promising approach is neither local law nor a new international covenant, but rather a strong, enforceable code of conduct created by the corporations themselves, in concert with nongovernmental organizations (NGOs), academics, states, and other stakeholders.

Control of the information and communication technologies environment

We are still in the early stages of the struggle for control on the Internet. Early theorists, citing the libertarian streak that runs deep through the hacker community, suggested that the Internet would be hard to regulate.[1] "Cyberspace" might prove to be an alternate jurisdiction that the long arm of the state could not reach. Online actors, the theory went, would pay little heed to the claims to sovereignty over their actions by traditional states based in real-space.

An emerging trajectory: More state control, greater pressure on private parties

As it turns out, states have not found it so very hard to assert sovereignty where they have needed to do so. The result is the emergence of an increasingly balkanized Internet, and the theory of "unregulability" no longer has currency. Many scholars have described the present-day reality of the reassertion of state online control, despite continued hopes that the Internet community itself might self-regulate in new and compelling ways.[2]

The dynamic of online control has changed greatly over the past 10 years, and it is almost certain to change just as dramatically in the 10 years to come. The "technologies and politics of control" of the Internet, as Jonathan Zittrain has put it, remain in flux.[3] Members of the Internet Governance Forum (IGF), chartered via the process that produced two instances of the World Summit on the Information Society (WSIS), continue to wrestle with a broad set of unanswered questions related to control of the online environment. At a simple level, the jurisdictional question of who can sue whom (and where that lawsuit should be heard, and under the law of which jurisdiction the conflict should be adjudicated, for that matter), remains largely unresolved, despite a growing body of case law. A series of highly distributed problems—spam, spyware, online fraud—continues to vex law enforcement officials and public policymakers around the world. Intellectual property law continues to grow in complexity, with some degree of harmonization underway among competing regimes. Each of these problems leaves many unresolved issues of global public policy in its wake.

A key aspect of online control—and one that is empirically proven through the work of ONI—is that states have, on an individual basis, defied the cyber-libertarians by asserting control over the online acts of their own citizens in their home state. The manner in which this control is exercised varies. Sometimes the law bans citizens from performing a certain activity online, such as accessing or publishing certain material. Sometimes the state takes control into its own hands by erecting technological or other barriers within the state's confines to stop the flow of bits from one recipient to another. Increasingly, though, the state is turning to private parties to carry out the online control. Many times, those private parties are corporations chartered locally or individual citizens who live in that jurisdiction. The emphasis of this chapter is yet another instance, in which the state requires private parties—often intermediaries whose services connect one online actor to another—to participate in online censorship and surveillance as a cost of doing business in that state.[4]

Legitimate state online control

The need for states to be able to exercise some measure of online control is broadly accepted. Likewise, states ought to be able to provide rights of action—ordinarily, the right to sue someone—to their citizens to enable them to seek redress for harms done in the online environment. That presumption is not challenged in this chapter. The easiest, perhaps most universal case is the common abhorrence of child pornography. Most societies share the view that imagery of children under a certain age in a sexually compromising position is unlawful to produce, possess, or distribute. The issue in the context of child pornography is less whether the state has the right to assert control over such material, but rather the most effective means of combating the problem it represents and the problems to which it leads without undercutting rights guaranteed to citizens. The prevention of online fraud or other crimes, which often target the elderly or disadvantaged, likewise represents a common purpose for some measure of state control of bits online. Some would argue that intellectual property protection represents yet another such example, though the merits of that proposition are hotly contested.

Where the state cannot effectively carry out its mandate in these legitimate circumstances, the state reasonably turns to those best positioned to assert control of bits. Often, though not always, the state turns to Internet service providers (ISPs) of one flavor or another. The law enforcement officer, for instance, calls upon the lawyers representing ISPs to turn over information about users of the online service who are suspected of committing a common crime, such as online fraud. As criminals use the Internet in the course of wrongdoing, states need to be able to access the increasingly useful store of evidence collected online.

The strongest form of this argument is that online censorship and surveillance is a legitimate expression of the sovereign authority of states. Saudi Arabia, for instance, which implements one of the most extensive and longest-running filtering regimes, did not introduce Internet access to its citizens until the state authorities were comfortable that they could do so in a manner that would not be averse to local morals or norms. In particular, the Saudi regime has concerned itself with blocking access to online pornography, which it has done with a startlingly high degree of effectiveness over the past five years. A state has a right to protect the morality of its citizens, the argument goes, and unfettered access to and use of the Internet undercuts public morality in myriad ways. Many regimes, including those in Western states (including the United States), have justified online surveillance of various sorts on the grounds of ordinary law enforcement activities, such as the prevention of domestic criminal acts. Most recently, states have begun to justify online censorship and surveillance as a measure to counteract international terrorism concerns, or more simply as the unalterable right of a state to ensure its national security. Whether or not states are right that they invariably have this sovereign authority is an open question—and beyond the scope of this chapter.[5]

Drawing a line: Where state online control implicates human rights standards

Some state-mandated acts of online control are not straightforward acts of local law enforcement. As the practice of online censorship and surveillance become more commonplace and more sophisticated, human rights activists and academics tracking this activity have begun to question whether some regimes of this sort violate international laws or norms. Quite often, the states that carry out online censorship and surveillance are signatories to international human rights covenants or have their own rules that preserve certain civil liberties for their citizens. The United States is home to a controversy of this sort, as the Electronic Frontier Foundation and others have filed a class action lawsuit against telecommunications giant AT&T for collaborating with the National Security Agency in a wiretapping program.[6]

The hardest puzzles are those cases where acts of local law enforcement seem to members of the international community to be violations of international norms. Consider a sovereign, jealous of its power, that disables access to opposition websites in the lead-up to an election—and then relents once the threat of losing control is abated. Or a state that routinely uses censorship and surveillance as a key element of a campaign to persecute a religious minority group. Or a state that relies upon online surveillance for the purpose of jailing political dissidents whose acts the state has committed to respect by international treaty. What about when a state is trying to protect public morals by keeping citizens from looking at garden-variety online pornography, but in so doing also block information on culturally sensitive matters, such as HIV/AIDS prevention or gay and lesbian outreach efforts?

What's at stake: Why Internet filtering and surveillance give rise to an ethical quandary

Just as states have a forceful claim to their right to exert sovereignty over their citizens, Internet censorship and surveillance prompt legitimate legal and normative concerns. The most straightforward of these concerns involve civil liberties. The online environment is increasingly a venue in which personal data are stored and across which personal communications flow. The basic rights of freedom of expression and individual privacy are threatened by the extension of state power, aided by private actors, into cyberspace. When public and private actors combine to restrict the publication of and access to online content, or to listen in on online conversations, the hackles of human

rights activists are understandably raised. Some argue that the right of free association is likewise violated by certain Internet censorship and surveillance regimes that are emerging around the world. Most complaints cite the Universal Declaration of Human Rights or the International Covenant on Civil and Political Rights as grounding ideals to which many states have agreed.

Even if one agrees with the strong form of the state sovereignty argument, and sets aside the notion that Internet censorship and surveillance can represent a violation of international laws and norms, one might still contend that these regimes are unwise or unethical. Internet censorship and surveillance, the technologist might argue, violate the "end-to-end principle" of network design. The end-to-end principle stands for the proposition that the "intelligence" of the network should not be placed in the middle of the network, but rather at the end-points. The extraordinarily rapid growth of Internet throughout the world is chalked up to this simple idea. By imposing control in the middle of the network—say, at the "great firewall" that surrounds China or proxy servers in Iran or at ISPs in dozens of states around the world—rather than at the user level, the censors will stymie the further growth of the network.

Jonathan Zittrain makes a related—but at once more subtle and more compelling—argument against unwarranted intrusion into online environments by pointing to the importance of "generative" platforms in the context of ICT. Rather than hewing to the original design of the network, he argues, the decision maker should favor those technical decisions that enable acts of innovation on top of the existing layers in the ecosystem—including not just those layers in the middle of the network, but also those at the edges. The kinds of individual creativity made possible by the personal computer (PC), including self-expression in the form of the creation of user-generated content, might be thwarted by the presence of a censorship and surveillance regime. The on-again, off-again blockage of the user-generated encyclopedia, Wikipedia, makes this case clearly. The sporadic use of filtering regimes to block the use of Voice over Internet Protocol (VoIP), often to protect the monopoly in voice communications of a local incumbent, also stands for this proposition.[7]

A third argument against the use of online censorship and surveillance regimes, and the participation of foreign technology companies in their instantiation, is the impact that these actions may have on the emergence of democracies around the world. The Internet has an increasing amount to do with the shape that democracies are taking in many developing states. The Internet is a potential force for democracy by increasing means of citizen participation in the regimes in which they live. The Internet can open the information environment to voices other than those organs of the state that have traditionally had a monopoly on the broadcast of important stories and facts, which in turn gives rise to what Fisher refers to as "semiotic democracy." The Internet can give a megaphone to activists and to dissidents who can make their case to the public, either on the record or anonymously or pseudonymously. The Internet can help make new networks, within and across cultures, and can be an important productivity tool for otherwise underfunded activists. Likewise, the Internet can function as a force for semiotic democracy—the notion that the control of cultural goods and the making of meaning are placed in the hands of many rather than few. Not least, the Internet is a force for economic development and the creation of a technologically sophisticated, empowered middle class, often in the form of local technology entrepreneurs. The Internet, in this sense, might function as a generative network in human terms, by helping to give rise to a more empowered citizenry.

New markets, new challenges

Technology, media, and telecommunications firms must decide whether to compete in markets where Internet censorship and surveillance are taking place against this contested backdrop. Internet filtering occurs in three regions of the world in particular: the Middle East and North Africa, Asia and the Pacific, and Central Europe and Asia. China continues to be the case that garners the most public attention, because of 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 three dozen states carry out some form of Internet censorship and surveillance online.

How Internet censorship and surveillance works

To add to the complexity of the matter, the mode and extent of censorship and surveillance varies substantially from one state to another. States rely upon a combination of types of controls to accomplish filtering and surveillance. The most apparent mode is through the use of technology. In its simplest form, the state places special code on computers that lie between the individual end-user and the broader network. The job of the code is to block certain data packets from reaching their destination or simply to learn and record the contents of those requests and who made them. Sometimes it is apparent to the end-user that his/her request for a certain Web page has been blocked by the state; 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—though, from the perspective of the state, it is not necessarily any harder to accomplish.

Online censorship (less so, surveillance) is carried out through nontechnical means as well. These controls are sometimes imposed by law: end-users are disallowed to

access or to publish certain information that is deemed to undermine public order or other state interests, for instance. The 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 through "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

For the purposes of this chapter, the most salient form of filtering is a combination of technical and legal control, trained on private actors with access to services that lie between an end-user and the network at large.[8] The state, unable to carry out filtering effectively on its own, requires private actors to carry out the censorship and surveillance for it. 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, the mandate from the state might be to ensure that search results provided to citizens of that state do not include links to online content that is banned in that jurisdiction. Likewise, the provider of a weblog-publishing tool might be prompted to include controls that disallow an individual publisher from including certain words in the title of a blog post. An Internet service provider might be required to keep records of the online activity of all or some of its subscribers, or to monitor the group of people who seek to access certain kinds of content. The provider of a Web-based email service might be required to turn over the email messages of a user suspected of a crime, or who is simply believed to be a member of the political opposition. The owner of a cybercafé, who is required to maintain logs of who uses what computers in their big open room, might be called upon to report on the identity of a certain Web surfer who used a given PC during a given time interval, or to call a special number on the fly if the online activity of a customer sets off certain alarm bells. The reach of the state is far greater in the online space when private actors can be enlisted to cooperate closely with the state's enforcers.

Two taxonomies of private actors facing this quandary

Different ICT-related 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 offer ways to disaggregate these firms. The first approach is to consider the type of business line of the firms, which is most useful for determining which firms might get drawn into an ethical controversy of this sort. The second, and more useful, taxonomy considers the nature of the involvement of the firms in the online censorship and surveillance regimes. The second taxonomy points the way forward more clearly toward a solution.

Types of firms

Several types of corporations might find themselves snared in this net. 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, as technologies and forms of digital content converge, other telecommunications service providers may well find themselves in a similar position.

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 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. Although nuclear technologies can provide energy efficiently to those who need it, it can also power weapons of mass destruction of previously 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 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 arguments similar 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 on the service providers who make the tools and update the lists. But, some observers suggest, the lists of banned sites include some NGOs that have no place there if the notion is just to protect children, for instance.

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, email service providers, blog-hosting firms, search engines, and others. ISPs are asked to route traffic in certain ways in order 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 are at once sensitive and potentially useful in the context of law enforcement activities. Email service providers are routinely asked to turn over information related to subscribers. The makers of weblog software and hosting services are asked to block certain information from being published and told to take down the postings or entire blogs of subscribers. Search engines 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.

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 are 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. Likewise, the notion of providing a single news or information service from one place in the world that is accessible from 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. Sometimes their content is filtered at the state level, but in those instances, the censorship is performed within the affected state. The ethical issue would arise only for those firms with local offices and offerings targeting a state that censors online material.

Telecommunications and other content delivery providers

On the horizon, one might imagine that additional classes of corporations could soon be drawn into this controversy. 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 VoIP services have already found that their services are sometimes blocked; 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 additional 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 makes the ethical questions come into greater relief than assessing simply the type of firm involved. 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 selling software or online services, including constantly updated block lists, that states use to implement their online censorship regime.
- **for surveillance**
  This category includes those firms that seek to profit

from selling 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 selling Internet-related hardware, including related software and services, that states use to implement their online censorship regime.
- **online surveillance**
  This category includes those firms that seek to profit from selling Internet-related hardware, including related software and services, that states use to implement their online surveillance regime.

Offering a service:

- **that is subject to censorship**
  This category includes those firms that seek to profit from providing 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.
- **that censors publication**
  This category includes those firms that seek to profit from providing online services that disallow a citizen of a state from publishing certain information online or that takes down previously published information at the behest of a state.
- **with personally identifiable information, subject to surveillance**
  This category includes those firms that seek to profit from providing 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 believe that they do not face a hard ethical question. For instance, in the case of an email service provider that turns over information to a law enforcement officer about a subscriber in a manner that prevents commission of a crime, the corporation may have few qualms about its actions. 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 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 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 a 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, 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 resolved cleanly. But absent such changes in the facts as they stand, the stakeholders who care about 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 would be for the relevant industries themselves to come up with a sustainable manner of ensuring that they operate ethically in these charged contexts. One or more groups of industry members might come up with a voluntary code of conduct that would govern the activities of individual firms in regimes that carry out online censorship and surveillance. This process would profitably include additional nonstate actors, such as NGOs and academics, as well as regulators with relevant expertise and authority. Corporations might further refuse to do business in regimes that put them in a position where they cannot comply with local laws while also honoring the voluntary code. Alternately, individual firms could come up with their own principles, much like a privacy policy on today's Internet, with statements to clarify to users, shareholders, and others how the firm will

handle these situations. Last, an outside group might come up with a set of principles to which firms could be encouraged to subscribe, on the model of the Sullivan Principles and the Apartheid-era South Africa, and based upon which an institution might emerge to support the principles. As in the case of the Sullivan Principles, one or more states might ultimately take the principles and convert them into national law once they have reached a point of stability and acceptance.

The elements of such a code or set of principles might be general—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 a taxonomy of the second sort described above. 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.

A critical part of such a voluntary code would be either to enact them into law or to develop an institution charged with monitoring adherence to the code and enforcing violations. This institution—perhaps not a new institution, but a pre-existing entity charged with this duty—ought to include among its participants representatives of NGOs or other stakeholders without a direct financial stake in the outcome of the proceedings. This institution might or might 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 evolve.

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, though classic state regulation is unlikely to be the most effective means of addressing the 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 US 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 United States law if carried out in the home market. A "hands-tying" regulation of this sort might be combined with other approaches that might attack particular parts of the problem, but would be unlikely to 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 a difficult ethical position.

The reasons not to rely upon traditional legal mechanisms in this context are that such mechanisms will likely be blunt instruments and 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 statute or treaty may be equally hard-won. Laws fashioned in this fast-moving environment will function as a hopelessly trailing indicator. Law should be seen as a component of a solution, but not the primary approach.

International governance

Problems in cyberspace have rarely been solved by 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, perhaps with the exception of the role of the International Telecommunication Union (ITU) in related telecommunications contexts. The Internet Governance Forum, ably chaired by Nitin Desai and under the secretariat of Markus Kummer, has the authority to conduct an international dialogue on issues related to the information society. An international treaty process, though cumbersome, could emerge as the way ahead. Some activists have considered litigation under existing human rights agreements.

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 US Congress has held hearings on this matter in order 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 to shine a spotlight on corporate involvement in filtering and surveillance regimes. Although 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 information technology community to work together to develop a voluntary code of conduct, and possibly to enact that code into law over time. That code must be coupled with the establishment of a reliable mechanism for monitoring and compliance assurance, whether through traditional state-based enforcement or an

institution created for this purpose. 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 the NGO community at the table in a supportive, nonadversarial, mode. State regulators might also be drawn into the process in constructive ways. A process to establish such a code is well underway, with Google, Microsoft, Vodafone, and Yahoo! working with two dozen investor, human rights, and academic groups, such as the Center for Democracy and Technology, Business for Social Responsibility, and Amnesty International.[9] The affected industry need not—and ought not—go it alone.

Though the environment is too complex and unstable for the standard modes of law-making 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 in other locales could be counter-productive. The challenges inherent in framing the Global Online Freedom Act of 2006 and 2007, in the US context, point to some of the many the 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 than they are with what these corporations are doing at home should support these corporations as they seek to act responsibly in a complex global environment. That support might come in the form of state involvement and encouragement for participation in the voluntary code 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—by raising this issue in bilateral negotiations with key states, for example—to lessen the extent that corporations are placed in this position in the first place. 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. And states might enact laws that codify the principles that the industry comes up with through the collaborative process that is underway. But states alone are unlikely to be able to lead constructively and quickly enough to address this problem.

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 these obligations come 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 ICT 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. And multinational corporations have every incentive to work hard toward an industry-led, collaborative approach to resolving the tension in the meantime.

Notes

1 See Barlow (1996).

2 The trajectory of this struggle for control has been well documented. See, for example, Zittrain (2003) and Goldsmith and Wu (2006, pp. 65–86).

3 See http://cyber.law.harvard.edu/is02/ (last accessed December 26, 2006).

4 It has not yet been determined conclusively whether states would force foreign corporations to leave the jurisdiction for disobeying these edicts.

5 Note that Dutta and Jain (2006) consider, on p. 14, that "the number of Internet users in 2003 exceeds the number of personal computers on a global level, as compared to 1999, when the situation was reversed." To the extent that this phenomenon is due in part to shared Internet connections, such as cybercafés, (no doubt in addition to mobile devices, among other factors), these points of presence become increasingly important to the story of censorship and surveillance. It is worth noting that this chapter does not seek to address all forms of online control carried out by private parties at the behest of states: for instance, much online control is carried out by local firms, such as ISPs or cybercafés, that provide online services in their home markets.

6 See www.eff.org/legal/cases/att/ (last accessed December 26, 2006) for details about this lawsuit.

7 Consider the relevant arguments set out in "The Infrastructure Challenge in Telecommunications: A Role for Regulation," Chapter 1.2 of *The Global Information Technology Report 2006–2007*.

8 See Reidenberg (2004); see also Palfrey and Rogoyski (2006).

9 See www.socialfunds.com/news/release.cgi/7272.html for a full list of all groups involved as of January, 2007.

References

Barlow, J. P. 1996. *The Declaration of Independence of Cyberspace*. Available at http://homes.eff.org/~barlow/Declaration-Final.html (last accessed December 26, 2006).

Beardsley, S., L. Enriquez, M. Guvendi, M. Lucas, and A. Marschner. 2006. "The Infrastructure Challenge in Telecommunications: A Role for Regulation." *The Global Information and Technology Report 2005–2006: Leveraging ICT for Development*. Hampshire: Palgrave Macmillan. 25–37.

Dutta, S. and A. Jain. 2006. "Networked Readiness and the Benchmarking of ICT Competitiveness." *The Global Information and Technology Report 2005–2006: Leveraging ICT for Development*. Hampshire: Palgrave Macmillan. 3–24.

Fisher, W. W. 2004. *Promises to Keep: Technology, Law, and the Future of Entertainment*. Palo Alto: Stanford University Press. Chapters 1 and 6.

Goldsmith, J. and T. Wu. 2006. *Who Controls the Internet: Illusions of a Borderless World*. New York: Oxford University Press.

OpenNet Initiative. 2002–2007. Available at www.opennet.net.

Palfrey, J. and R. Rogoyski.. 2006. "The Move to the Middle: The Enduring Threat of 'Harmful' Speech to Network Neutrality." *Washington University Journal of Law and Policy* (21): 31–65.

Reidenberg, J. R. 2004. "States and Internet Enforcement." *University of Ottawa Law & Technology Journal* 1 (213): 213–30.

Zittrain, J. 2003. "Internet Points of Control." *Boston College Law Review* 44 (2): 653–88.