10 Corporate Accountability in Networked Asia

Rebecca MacKinnon

In 2010, Google's defiance of Chinese government censorship demands, followed by its decision to remove its Chinese search operations from mainland China, grabbed front-page headlines around the world. Human rights groups and socially responsible investors praised the global Internet giant for standing up to the Chinese government's censorship policies. China's sophisticated system of Internet censorship and control depends on the compliance of domestic and foreign corporate intermediaries, which are required by Chinese law to help authorities track user activity and to remove or prevent publication and transmission of politically sensitive content on or through their services.

Yet China is by no means the only Asian country where companies face government pressure to reveal user data or remove content in ways that violate internationally recognized human rights principles. Local and international human rights groups point to Vietnam, Burma, Thailand, and the Philippines as countries where "Chinese-style" Internet controls are increasingly deployed to silence or monitor dissent, often implemented by means of private-sector information and communication technologies (ICTs) service providers, carriers, and platforms.[1] Reporters Without Borders includes Thailand, Sri Lanka, Malaysia, Australia, and South Korea on its watch list of countries with surveillance trends heading in the wrong direction.[2]

Recent studies of global surveillance and censorship by the OpenNet Initiative (ONI) and others are showing that private-sector Internet and telecommunications companies play an increasingly important role in government efforts to control what citizens can or cannot do in cyberspace.[3] Even in Asia's most vibrant democracies such as South Korea and India, companies—domestic and foreign—face government demands for censorship and user-data handover in ways that violate Internet users' rights to free expression and privacy.

The idea that upholding free expression and privacy rights should be a component of "corporate social responsibility" (CSR)—alongside other corporate responsibilities including labor standards, environmental protection, and sustainability—is a new concept for nongovernmental organizations (NGOs), investors, companies, and

governments in the industrialized West, let alone anywhere else.[4] In the first ONI volume, *Access Denied*, Jonathan Zittrain and John Palfrey called for an industry code of conduct.[5] In 2008 came the launch of the Global Network Initiative (GNI), a multi-stakeholder initiative through which companies not only make a commitment to core principles of free expression and privacy, but also agree to be evaluated independently on the extent to which they actually adhere to these principles.[6] In the second ONI volume, *Access Controlled,* Colin Maclay examined the challenges facing this newly formed organization, a core challenge being the recruitment of members.[7] As of this writing, only three companies, Google, Microsoft, and Yahoo!, have agreed to be held publicly accountable for the way in which they handle government demands for censorship and surveillance around the world. No other North American companies have made this public commitment, and no companies from any other continents or regions have yet been willing to make a similar public commitment to free expression and privacy as a core component of responsible business practice.

Yet other forms of CSR—including environmental, labor, and sustainability standards—are by no means foreign to Asian businesses, even in China.[8] Might public expectations for corporate accountability in the area of free speech and privacy also rise in Asia in the coming years—particularly if these expectations are fed by increased civil society activism, pushing for greater accountability and transparency by ICT companies around their interactions with governments? In this chapter I compare government censorship and surveillance demands faced by companies in authoritarian China alongside the challenges faced by companies in two neighboring democracies that also have robust ICT industries and markets: South Korea and India. I argue that efforts to hold companies other than Google, Yahoo!, and Microsoft accountable for free speech and privacy in authoritarian countries like China will face an uphill battle unless companies in Asia's democracies are pushed by domestic civil society actors to defend and protect user rights in a more robust manner than is currently the case.

China: "Networked Authoritarianism" and the Private Sector[9]

As ONI research over the past decade has shown, China has the world's most sophisticated system of Internet filtering, which blocks access to vast numbers of Web sites and online content hosted by companies and on computer servers located mainly outside China.[10] But filtering is only the top layer of the country's elaborate system of Internet censorship. For Web sites run by individuals or companies located inside China, the government has direct jurisdiction—and thus more powerful instruments of control. Why merely filter a Web page when you can get it removed from the Internet completely or prevent its publication or dissemination in the first place? Over the past decade as Internet penetration grew rapidly in China, government regulators

have created strong negative incentives—including Web site registration requirements, the threat of jail sentences for individuals, and the cancellation of business licenses for companies—in order to keep certain kinds of content off the Internet.[11] Ronald Deibert and Rafal Rohozinski classify this approach to censorship as "second-generation Internet controls."[12] The Chinese government calls the system corporate "self-discipline," and hands out an annual award to companies that have done the best job of keeping their Web sites "harmonious" and free of sensitive content—ranging from the pornographic to the political.[13]

In Anglo-European legal parlance, the legal mechanism used to implement such a "self-discipline" system is a form of "intermediary liability."[14] It is the legal mechanism through which Google's Chinese search engine, Google.cn, was required to censor itself until Google redirected its simplified Chinese search engine offshore to Hong Kong.[15] All Internet companies operating within Chinese jurisdiction—domestic or foreign—are held liable for everything appearing on their search engines, blogging platforms, and social-networking services. They are also legally responsible for everything their users discuss or organize through chat clients and messaging services. In this way, much of the censorship and surveillance work is delegated and outsourced by the government to the private sector. If private companies fail to censor and monitor their users to the government's satisfaction, they will lose their business licenses and be forced to shut down.[16] All large Internet companies operating in China have entire departments of employees with hundreds of people whose sole job is to police users and censor content around the clock.[17]

Companies are also expected to play a role in the surveillance of Internet and mobile users. In a country like China where "crime" is defined broadly to include political dissent, companies with in-country operations and user data stored locally can easily find themselves complicit in the surveillance and jailing of political dissidents. The most notorious example of law enforcement compliance gone very wrong was when Yahoo!'s local Beijing staff gave to the Chinese police e-mail and user-account information of journalist Shi Tao, activist Wang Xiaoning, and at least two others engaged in political dissent.[18] There are other examples of how law enforcement compliance by foreign companies has compromised activists. In 2006, Skype partnered with a Chinese company to provide a localized version of its service, then found itself being used by Chinese authorities to track and log politically sensitive chat sessions by users inside China. This happened because Skype delegated law enforcement compliance to its local partner without sufficient attention to how the compliance was being carried out. The local partner, in turn, was merely following standard industry practice that is commonplace for domestic Chinese Internet companies.[19]

In this way, the private sector in China plays a key role in a political innovation that I call "networked authoritarianism."[20] Compared to classic 20th-century authoritarianism, this new form of Internet-age authoritarianism embraces the reality that

even when extensive filtering regimes are put in place, people cannot be prevented from accessing and creating a broad range of Internet content and holding all kinds of conversations, including those related to politics and policy. Networked authoritarianism thus accepts and allows a lot more give and take between government and citizens than in a pre-Internet authoritarian state. The regime uses the Internet not only to extend its control but also to enhance its legitimacy. While one party remains in control, a wide range of conversations about the country's problems rage on Web sites and social-networking services. The government follows online chatter and sometimes people are able to use the Internet to call attention to social problems or injustices, and even manage to have an impact on government policies. As a result, the average person with Internet or mobile access has a much greater sense of freedom—and may even feel like he or she has the ability to speak and be heard—in ways that were not possible under classic authoritarianism. It also makes most people a lot less likely to join a movement calling for radical political change. Meanwhile, the government exercises targeted censorship focused on activities and conversations that pose the greatest threat to the regime's power, and also devotes considerable resources to proactively seeding and manipulating the nation's online discourse about domestic and international events.[21]

Thus, while over 500 million Chinese people are finding their lives greatly enhanced by the Internet, Communist Party control over the bureaucracy and courts has strengthened, and the regime's institutional commitments to protect the universal rights and freedoms of all its citizens have weakened.[22] According to a recent report by the Dui Hua Foundation, in 2008 arrests and indictments on charges of "endangering state security"—the most common charge used in cases of political, religious, or ethnic dissent—more than doubled for the second time in three years.[23] Meanwhile, the Chinese government has made clear in its 2010 Internet White Paper that the rapid nationwide expansion of Internet and mobile penetration is a strategic priority. The development of a vibrant indigenous Internet and telecommunications sector is critical for China's long-term global economic competitiveness.[24] At the same time, Chinese companies are fully expected to support and reinforce domestic political stability, and to ensure that ICTs will not be used in a manner that threatens Communist Party rule.[25]

The China case demonstrates how companies can be used as an opaque extension of state power, helping authoritarian regimes to control and manipulate citizens with a lighter hand than was possible in the pre-Internet age while still maintaining power and preventing viable opposition movements from emerging. But what about democracies? In democratic societies, can ICT companies be used as an opaque tool for incumbent leaders, ruling political parties, and other powerful groups to manipulate public discourse and marginalize critics? Trends in South Korea and India suggest that such a situation is possible and may already be happening to different degrees. To

prevent creeping networked authoritarian tendencies in democratic societies, stronger strategic alliances between civil society and industry will be needed to push back against abuse of government power by means of digital networks and platforms.

South Korea: From Dictatorship to E-Democracy to "Free-Floating Control"[26]

After decades of dictatorship, South Korea underwent a successful transition to democracy in the 1990s. At the same time, thanks to a strong government emphasis on ICT investment over the past two decades, by 2009 more than 80 percent of South Koreans had become Internet users, with Internet access reaching more than 95 percent of households.[27] Upon his inauguration in 2003, late President Roh Moo-hyun was hailed in the international media as the world's first "Internet president" of the world's most advanced "Internet democracy."[28] His narrow election victory was widely credited to viral mobilization by his online supporters via citizen-media Web sites like OhmyNews.[29] Yet by 2009 domestic and international human rights groups were sounding the alarm about mounting and blatant violations of Korean citizens' right to free expression and privacy on the Internet.

In March 2010, Reporters Without Borders placed South Korea on its watch list, citing "a liberticidal legislative arsenal that is inducing netizens to practice self-censorship—all that in the name of the fight against dissemination of 'false information.'"[30] After visiting South Korea in May 2010 and meeting with local human rights organizations as well as government officials, the United Nations special rapporteur on freedom of expression, Frank La Rue, concluded, "I am concerned that in recent years, there has been a shrinking space for freedom of expression in the Republic of Korea." Online expression, he wrote in a press statement, was being squeezed by "arbitrary procedures for the deletion of information on the Internet" as a result of the broadening of regulatory requirements placed on Internet service providers (ISPs) and other content-hosting services.[31] He also cited South Korea's real-name identification requirement for Internet portals, which he concluded "has the potential to undermine individuals' right to express opinions, particularly criticisms of the Government, as well as the right to privacy."[32]

Laws requiring real-name registration tied to the National ID system for all users of Internet portals and services over a certain size, as well as other laws targeting "spread of rumors," defamation, and "campaigning" during an election period, were first enacted during the Roh administration.[33] The reasons for their enactment are familiar to many democratic societies in the Internet age: protecting innocent people against cyber harassment, cyber bullying, and cyber attack. By the middle of the first decade of the 21st century, cyber bullying had become a serious social problem in Korea: vicious cyber mobs had caused the suicide of several celebrities and turned ordinary citizens into national pariahs for being caught on cell-phone cameras

engaging in offensive yet relatively common behavior.[34] South Korean government, industry, and society at large were by 2003 already beginning to feel the cost of sophisticated cyber attacks.[35] A 2006 poll revealed that 85 percent of South Korean high school students were under stress from cyber bullying.[36] Real-ID requirements on Internet platforms and enhanced surveillance capabilities were touted by policymakers as a solution to social problems and crimes that the Internet had enabled, amplified, and exacerbated.

However, South Korean human rights activists argue that since the current president, Lee Myung-bak, took office in 2008, government measures have had an increasingly adverse impact on free expression and privacy. The ruling party, they say, has used media and communications laws to maximize its own political advantage, resulting in a marked "chilling effect" on political speech.[37] Measures include deletion or "temporary blocking" of Internet postings that criticize the government and powerful individuals, and prosecutions of individuals for dissemination of information characterized as "false communication using electronic communication facilities for the purpose of derogating public interest."[38] Laws against dissemination of false information, combined with the real-name registration requirement for all Internet services with more than 100,000 visitors per day, have resulted in the identification and prosecution of a number of Internet users for speech that is supposed to be protected under international human rights norms. Examples include the arrest of a teenager who proposed a student strike on a popular forum, and the arrest of the influential economic commentator known as "Minerva" for posting articles critical of the government's currency policy.[39] The man who wrote pseudonymously as "Minerva," Park Dae-sung, was identified by government investigators because the Internet portal Daum was required by law to hand over records of the account holder's real identity and National ID number. He was eventually acquitted, but only after spending five months in jail. Human rights groups argued that his experience has had a chilling effect on other citizens who might otherwise be motivated to post critiques of government policies online.[40] In December 2010, South Korea's Constitutional Court ruled that the telecommunications law banning the spread of false information was unconstitutional, citing unclear definitions in the law of terms such as "false" and "public interest."[41] While this ruling was hailed by digital rights groups as a major victory, other laws, including the real-ID requirements, remain in force.

While the Internet initially had a politically disruptive and democratizing effect on South Korean politics, enabling a political insurgent to win election in 2002 by circumventing political narratives promoted by mainstream broadcast and print media, the Internet has been used by the current regime as part of its efforts to chill dissent and marginalize critics.[42] Scholar Kwang-Suk Lee describes this process as an evolution from a dictatorship reliant on centralized, hierarchical control to a democracy whose political establishment seeks, through laws passed by a democratically elected

legislature, to develop a new "distributed and ubiquitous network model" of governance and manipulation of the public discourse, enabled by "positive technologies for free floating control" which "can hide under an ethical patina the real intention of control directed at establishing the new digital rule of cybersociety."[43]

In 2009, Google decided that it would not contribute to this trend. In April of that year the company announced that the local Korean section of its video-sharing service, YouTube, would disable users from uploading videos or posting comments because allowing them to do so without registering their real names and ID numbers was a violation of local law. The company cited a concern for South Korean Internet users' right to freedom of expression, stating on its official blog, "We believe that it is important for free expression that people have the right to remain anonymous, if they choose."[44]

Unnamed executives quoted in the press at the time indicated that South Korean companies resent being used as agents for the chilling of free expression in their country, but find themselves in a weaker position to resist given that their main customer base—and in many cases sole market—is domestic. In the wake of Google's announcement, The Hankyoreh news Web site quoted an unnamed executive at one of South Korea's major Internet portals who said, "When I saw Google's decision, I was jealous and at the same time deeply distressed. . . . South Korean businesses will have to endure criticism from users while following unwanted regulations."[45] The *Korea Times* quoted a similarly frustrated official from Daum, the country's second-largest Web portal: "The increasing government regulations can't help Korean Web portals if Internet users feel they're on a short leash. Korea is one of the few countries where local companies introduced enough quality services to stay ahead of global Internet giants in the market, but now it seems we may be losing some of our competitive edge."[46]

In China, where there is little hope of a fair hearing in the courts, no free media coverage, and no recourse to oppositional politics, executives can ill afford to stand up to the government. However, South Korean companies, operating in a democracy, are in a much stronger position to advocate on behalf of the rights of their users, challenge government orders in cases that are arguably unconstitutional or even illegal, and push for changes in law so that they will not be compelled to act as de facto opaque extensions of the ruling political power in a way that taints their own relationship with users and customers.

It appears that at least some attempts are being made in this direction. In April 2009, the *Korea Times* reported that K-Internet, an industry lobby of 150 Internet companies, protested against a controversial bill proposed in parliament by members of the ruling Grand National Party that would grant intelligence authorities greater powers to intercept user communications on mobile telephone networks and Internet services, requiring all ICT companies to maintain comprehensive logs of user and

customer communications. K-Internet argued that the bill "seems to be focused excessively on improving the 'efficiency' of investigations and less on protecting communication freedoms and limiting threats to privacy, posing a serious threat to the fundamental rights of citizens, limiting the business of communications operators and needlessly increasing social costs." An "industry insider" was further quoted as saying, "There is no fun in joking about Pakistan and China anymore, when our own government seems to have a similar approach to Internet users."[47] Korean ICT companies clearly see a link between protecting users' and customers' rights and their long-term brand reputation and commercial success. It is less clear whether civil liberties groups and Korean businesses are seeking or finding ways to work together effectively, not only to prevent further incursion but also to regain lost ground.

India: Systematizing Surveillance[48]

In contrast to South Korea's 82 percent Internet penetration as of 2009, India's Internet penetration hovered around 5 percent. While small in percentage terms, that still translates into nearly 60 million Internet users—larger than South Korea's roughly 40 million.[49] More broadly, India's telecommunications market is the fastest growing in the world, with industry executives predicting that the number of Indian mobile phone users could surpass one billion by 2015.[50] While India has a lively blogosphere and large communities on Orkut, Facebook, and Twitter, Indian citizens also expect their government to protect them from the spread of online crime, shield youth from pornography in a country where traditional values remain important, and take measures to prevent ethnic and religious violence in a country with a highly complex and volatile mix of religions and ethnicities. Internet and mobile technologies were used to coordinate the 2008 Mumbai terrorist attacks.[51] Cyber attacks launched from China, uncovered in 2009, exposed the need for improved cyber security.[52] Although these are all serious concerns for any democracy in the Internet age, the Indian government's approach to addressing these problems has raised concerns from civil liberties groups and industry.

The Information Technology Act of 2000 established the legal framework for filtering and regulating India's Internet, as well as the procedures by which ISPs and other Internet content and service companies can be compelled to censor online material or share information with government authorities.[53] Several incidents took place in the early 21st century in which the government ordered ISPs to block specific blogs and groups hosted on international services like Orkut, Yahoo Groups, and Blogger. These filtering efforts proved counterproductive because ISPs lacked the technical capacity to block individual subdomains, resulting in the blanket blocking of Blogger, Yahoo Groups, and Orkut at different points in time. This in turn prompted widespread public outcry and ridicule in the Indian media and blogosphere. It also sparked

grassroots efforts to spread knowledge among Indian Internet users about circumvention technologies so that most people who really wanted to access the offending content could still manage to do so.[54]

By the end of the decade the Indian government had changed its strategy for dealing with problematic content posted on, or transmitted through, the services of Internet companies. Ham-fisted and overbroad ISP-level filtering gave way to direct demands to the companies themselves to hand over user data and delete content.[55] The Information Technology (Amendment) Act of 2008 facilitated this transition by empowering the state to direct any ICT service to block, intercept, monitor, or decrypt any information through any computer resource.[56] The act also requires companies to have a designated point of contact for content-blocking, removal, and data requests. Company officials who fail to comply with government requests can face fines and up to seven years in jail.[57] Analysts point out that the new act has made ISP-level filtering more difficult, while strengthening and systematizing surveillance processes.[58] While most critics acknowledge the legitimate role of law enforcement, they have called for more comprehensive rules and procedures to supervise the process by which government demands are made, in order to prevent privacy violations, foul play, and political abuse.[59]

It was against this backdrop in early August 2010 that the Indian government demanded that Research in Motion (RIM), maker of Blackberry smart phones, grant Indian security agencies access to all corporate e-mail and instant-messenger communications transmitted within or through Indian borders. Failure to comply by the end of the month would result in blockage of all encrypted Blackberry traffic on Indian networks.[60] Gaining access to Blackberry's consumer services sold locally over domestic mobile carriers was one thing, and RIM expressed willingness to help the Indian government in this regard.[61] However, given that even RIM itself cannot access user data on Blackberry Enterprise Services—it is transmitted in highly encrypted form and retained on the corporate customers' servers—full compliance with the government's order in its original form is difficult if not impossible.[62] The company reportedly offered Indian authorities manual access to its messenger service with a pledge of real-time automated access by early 2011 and gained a reprieve from punishment until that time.[63]

Indian authorities claim to have begun conversations with other global companies, including Google and Skype, neither of which would comment publicly because they say they had not yet received any formal government requests or orders. Meanwhile, by late 2010 concerns were mounting in the Indian business community about the economic implications of their government's threats.[64] "We need a more balanced approach for lawful interception," wrote S. Ramadorai, vice chairman of Tata Consultancy Services Limited. "Bans and calls for bans aren't a solution. They'll disconnect India from the rest of the world. We can't allow that to happen, because then terrorists will win without even firing a bullet."[65]

Google has demonstrated that while companies are not in a position to commit civil disobedience if they want to stay in a market, they may be able to contribute to greater accountability by releasing more information about the demands that government authorities are making and whether they have been complied with. In September 2010, Google released a transparency report showing that from January through June, the Indian government made 30 content-removal requests (totaling 125 items), 53.3 percent of which Google claims to have "fully or partially complied with." Fourteen hundred and thirty Indian government requests to Google for user data ranked India the third highest in the world (behind 2,435 by Brazil and 4,287 by the United States)—not counting China.[66] The number of requests made by the Indian government to other foreign or domestic operators is unknown.

The Google Transparency Report has brought up some interesting questions. What if other multinational companies operating in India, along with Indian companies, all released similar data? Would that provide concerned citizens with at least some of the ammunition they need to hold their government accountable and ensure that censorship and surveillance in a democracy are restricted to the absolute minimum needed to protect innocent citizens' lives when they are clearly endangered by specific online activities by specific individuals, and that these tactics are not being abused for broader political purposes? Should India's vibrant activist community mount a campaign demanding that all companies operating in India must release similar transparency reports? Might they even lobby for the passage of a law requiring it? Might that at least be a first step toward necessary accountability?

Indian digital rights activists worry that India's vibrant nongovernmental sector has failed to mobilize on issues of digital free expression and privacy. In 2003, Supreme Court advocate Pavan Duggal wrote, "There is a need to change people's mindset [where most] view IT in isolation to democracy."[67] The problem does not seem to have improved over the decade. In 2007 lawyer Raman Jit Singh Chima lamented an "apparent lack of interest amongst traditional Indian civil liberties organizations in anything to do with the Internet or digital civil liberties in general."[68] In a 2009 report summarizing the state of Internet rights in India, activists Gurumurthy Kasinathan and Parminder Jeet Singh concluded that "unfortunately, in India, while different groups engage with some of the issues . . . in a piecemeal manner, there is little recognition of how they connect and reinforce each other in the building of a new social paradigm—euphemistically called an *information society*—that may require a set of coordinated civil society responses."[69]

Even in China, business leaders have expressed concern in private and semipublic forums that excessive burdens imposed on companies by governments can adversely impact innovation, which ultimately hurts national competitiveness.[70] The nature of China's legal and political system, however, makes it nearly impossible for Chinese companies to challenge government demands in the courts, take the debate to the

court of public opinion through the media, or make common cause with civil liberties activists. Their position is made even weaker, unfortunately, when neighboring democracies like India and South Korea—and many other democracies around the world—set legal, technical, and regulatory precedents for government-directed censorship and surveillance to be built within privately operated digital networks without sufficient public oversight, transparency, and accountability. Chinese media frequently cite South Korean examples in particular when arguing that China's Internet controls are in line with international practice.[71]

Corporate Social Responsibility

While it may be easier said than done, the idea of CSR—the notion that long-term corporate success requires the inclusion of environmental, sustainability, and human rights concerns in companies' core technologies, management, and business practices—is being embraced by publics around the world.[72] John Ruggie, special representative of the secretary-general of the United Nations on business and human rights, in examining how companies can and should be expected to contribute to human rights around the globe, concluded that while human rights are primarily the responsibility of the nation-state, companies must also respect, protect, and uphold internationally recognized human rights norms in the spheres of human life and activity over which their business exerts influence or on which it has an impact.[73] The problem is that most companies do not have systems or procedures in place to identify when they are doing harm, let alone processes to anticipate harm done by new business activities and technologies. The core work of genuine corporate social responsibility involves building such systems and mechanisms. Doing so generally requires working with outside stakeholders including environmental, labor, and human rights activists, socially responsible investors, industry groups, and governments.[74]

Concepts of CSR and "sustainable business" are taking root around Asia, albeit in different forms and guises in different Asian countries, given the region's tremendous variation in cultural, political, and economic contexts.[75] More Asian countries are shifting from a focus on labor-intensive manufacturing and export-oriented growth strategies. Governments around the region are placing growing emphasis on innovation in services, technology, and knowledge sectors as the key to economic growth and national competitiveness. The "knowledge-based corporation" is critical to South Korea's continued economic success and is considered by the Chinese and Indian governments to be an important driver of their nations' economic futures. Such companies have few tangible assets and rely heavily on intellectual property, innovative processes, and public reputation. Experts in business management point out that "reputational capital" is difficult to build and easy to lose, making it all the more

important that such companies anticipate and seek to avoid problems that could damage their reputation and lead to loss of "legitimacy" with their target users and customers.[76]

In India, the idea that business has a duty to serve the greater social good has deep roots in Gandhi's "trusteeship" model.[77] The Tata Group, which owns a number of ICT-related businesses, proudly quotes its founder Jamshetji Nusserwanji Tata (1839–1904): "In a free enterprise, the community is not just another stakeholder in business, but is in fact the very purpose of its existence."[78] While Indian companies have traditionally equated "corporate social responsibility" with charitable donation, a growing number—pushed by a broad range of civil society groups from national and international NGOs to local grassroots movements—are recognizing the need to engage with a broad range of "stakeholders" affected by their business, including India's many vibrant NGOs and grassroots activist groups, representing the interests of affected communities and groups.[79] As Indian multinationals expand around the world and seek to sharpen their competitiveness, more of them are adopting international standards for corporate social responsibility in order to improve their reputational capital in foreign markets.[80]

In South Korea, research shows that consumers tend to reward companies with reputations for being "good" to their communities and to their workers, while being less inclined to base purchasing decisions on companies' environmental practices.[81] Yet the South Korean environmental movement, which blossomed after the political system democratized in the early 1990s, achieved substantial change through public campaigns, media tactics, and political strategy. Most importantly, over the course of two decades the South Korean environmental movement—with the support of a broader global movement—was successful in reframing national priorities and values away from an earlier "developmentalist" narrative, promoted by government and industry, that economic development should be achieved at all costs.[82] Over time, thanks to democratization and greater media freedoms, the public and policymakers alike came to embrace the notion that clean soil, air, and water and conservation of national resources were not only essential for people's health and well-being, but were ultimately necessary for the nation's continued economic success. This shift in values has been crucial to bringing about change in government policy and business practice.[83]

South Korean society—like all modern industrialized consumption-driven economies—struggles with the problem of how to truly walk the talk. But the critical first step was to reframe prevailing narratives of what national "success" should look like. Globally, the mounting public pressure on companies to act responsibly is due to a dramatic shift in public expectations. That, in turn, is thanks to civil society's success in reframing the public discourse. Again, implementation remains a constant struggle. But once the concept was firmly planted in the public consciousness, it took root and has continued to grow.

In China, corporate social responsibility has been driven primarily by government fiat, based on the urgent recognition that environmentally sustainable business practices are imperative for the nation's long-term competitiveness as well as its people's physical survival. In January 2008, China's State-Owned Assets Supervision and Administration Commission decreed that "Corporate Social Responsibility has become a key criterion worldwide when people assess the value of a company."[84] Chinese companies were ordered to adopt global best practices so that their value for investors would rise. The number of Chinese companies producing sustainability reports shot up—from a handful in 2006 to more than 600 by 2009. By 2010 more than 600 companies were also participating in the United Nations Global Compact.[85] An ICT company—China Mobile—became the first mainland Chinese company to meaningfully disclose its carbon dioxide emissions, and it was also the first to be listed on the Dow Jones Sustainability Index.[86] While it would be difficult to imagine China Mobile signing on to the Global Network Initiative principles of free expression and privacy in China's current political climate, it is significant that Chinese companies—and Chinese policymakers—now view adherence to global CSR standards and expectations as an important part of Chinese companies' investment value. Such changes point to some reason for hope in the event that free expression and privacy become a more mainstream and established component of CSR for corporations, socially responsible investors, and civil society groups in the world's industrialized democracies.

Conclusion

Asia's governments—like all governments around the world—are grappling with many difficult challenges that the Internet has created for law enforcement and national security. Meanwhile, not only do civil society groups face new issues in terms of learning and deploying all the latest digital technologies for advocacy and discourse, but activists also have to keep developing new strategies, new knowledge, and new capacities in the fight to preserve civil liberties in the digital realm.

There are many questions to which nobody yet has answers. How can free expression and privacy be integrated into public definitions and expectations of responsible business behavior? What will it take for a critical mass of ICT companies operating in Asia to become more assertive in defending users' rights to free expression and privacy? What will it take to compel more multinational companies beyond the three GNI members, Google, Yahoo!, and Microsoft, to stand up for their users' rights to free expression and privacy not only because it is the right thing to do but also because they understand that in the long run this is the most successful business strategy?

In *Big Business, Big Responsibilities: From Villains to Visionaries: How Companies Are Tackling the World's Greatest Challenges,* authors Andy Wales, Matthew Gorman, and

Dunstan Hope point out that the issues of free expression and privacy involve relationships between citizens, companies, governments, and laws that are different from "traditional" CSR issues. In the case of environmental and labor practices, for instance, citizens often work with governments to force companies to stop polluting or improve treatment of workers, through the passage and enforcement of laws. However when it comes to government-driven incursions on free expression and privacy by means of censorship and surveillance, the problem lies with domestic laws, regulations, or law enforcement practices that are not in line with international human rights norms. Thus a "common cause" between citizens and companies is necessary in order to achieve the desired goal of protecting citizens' rights from the potential abuse of government power. "What we are witnessing," they observe, "is an intriguing alliance between the user and the company in defense of human rights."[87]

Environmental-protection and labor rights groups in countries such as South Korea and India have historically had good reason to view corporations as adversaries whose pursuit of profit has resulted in environmental degradation and human exploitation. Democratically elected government is won over by civil society as an ally in imposing standards and rules on the private sector. When it comes to Internet surveillance and censorship, however, interests are aligned in a different way so that citizens need corporate-owned digital intermediaries to help shield them from abuses of government power. Companies can do this by challenging—or at the very least publicly exposing—government demands for censorship and surveillance, which, if not arguably unconstitutional or illegal according to domestic law, clearly infringe on rights enshrined in the Universal Declaration of Human Rights and other international covenants.

Finding common cause *with* the private sector *against* government abuse of citizen rights does not come naturally to many civil society activists in Asia's democracies, many of which have only recently emerged either from corporatist-authoritarian pasts or from centralized systems of economic planning. As digital rights activists quoted earlier in this chapter pointed out, joining forces with the business community is not consistent with the anticapitalist culture of many Indian civil society groups. Similarly, South Korean civil society groups came of age in a culture of often-violent labor protest against corporate *chaebols* with close ties to the regime. Corporate managers have equally large cultural and mental barriers preventing them from tapping the moral force of civil society groups, who can potentially be powerful allies in helping companies stave off government interference of the sort that is likely to hamper their ability to innovate and compete on a global scale.

Achieving common cause between civil society and business thus requires new thinking, new attitudes, and new strategies on all sides. While these innovations will not be accomplished easily, in countries where civil society and business succeed in

working together to promote transparent and accountable governance of digital networks, the result could be a win-win for citizens' rights *as well as* high-tech competitiveness. Multinational companies from India and South Korea might even gain a competitive and reputational edge with global customers by joining the Global Network Initiative—even ahead of many of their European and North American competitors.

Studies of CSR practices in Asia show that even in democracies, managers and investors prefer to avoid terms like "human rights" and "social justice," which tend to be culturally associated with Western-style moralism. Instead, proponents and practitioners of CSR in Asia tend to emphasize concepts like "sustainability," with a strong emphasis on why environmental and labor standards contribute positively to social stability as well as companies' long-term value.[88] Such arguments have proven economically compelling even to corporations and regulators in authoritarian regimes such as China. If civil society and businesses in Asia's democracies can successfully make the economic value case for upholding global standards for free expression and privacy in the governance of digital networks, and if ICT companies from those nations gain a competitive boost as a result, there may well be reason to be optimistic that something similar may even happen in China someday.

Notes

1. Ben Doherty, "Silence of the Dissenters: How South-east Asia Keeps Web Users in Line," *The Guardian,* October 21, 2010, http://www.guardian.co.uk/technology/2010/oct/21/internet-web-censorship-asia.

2. Reporters Without Borders, "Web 2.0 Versus Control 2.0," March 18, 2010, http://en.rsf.org/web-2-0-versus-control-2-0-18-03-2010,36697.

3. Ronald Deibert and Rafal Rohozinski, "Liberation vs. Control: The Future of Cyberspace," *Journal of Democracy* 21, no. 4 (October 2010): 43–57.

4. "New Responsibilities in the Networked Age," in Andy Wales, Matthew Gorman, and Dunstan Hope, *Big Business, Big Responsibilities: From Villains to Visionaries: How Companies Are Tackling the World's Greatest Challenges* (New York: Palgrave Macmillan, 2010), 87–102.

5. Jonathan Zittrain and John Palfrey, "Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet," in *Access Denied: The Practice and Policy of Global Internet Filtering*, ed. Ronald J. Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2008), 103–122.

6. Global Network Initiative, http://globalnetworkinitiative.org.

7. Colin M. Maclay, "Protecting Privacy and Expression Online," in *Access Controlled: The Shaping of Power, Rights, and Rules in Cyberspace,* ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2010), 87–108.

8. "The Government of Big Business," in Wales et al., *Big Business, Big Responsibilities*, 119–124.

9. This section borrows heavily from Rebecca MacKinnon, "Networked Authoritarianism in China and Beyond: Implications for Global Internet Freedom," a paper presented at Liberation Technology in Authoritarian Regimes Conference, sponsored by the Hoover Institution and the Center on Democracy, Development, and the Rule of Law (CDDRL), Stanford University, October 11–12, 2010, http://rconversation.blogs.com/MacKinnon_Libtech.pdf.

10. OpenNet Initiative, "China: Country Profile," in *Access Controlled,* 449–487.

11. Rebecca MacKinnon, "Flatter World and Thicker Walls? Blogs, Censorship and Civic Discourse in China," *Public Choice* 134, nos. 1–2 (January 2008): 31–46.

12. Ronald Deibert and Rafal Rohozinski, "Beyond Denial: Introducing the Next Generation of Internet Controls," in *Access Controlled,* 3–13.

13. Rebecca MacKinnon, "Are China's Demands for Internet 'Self Discipline' Spreading to the West?" McClatchy Newspapers syndicated service, January 18, 2010, http://www.mcclatchydc.com/2010/01/18/82469/commentary-are-chinas-demands.html.

14. Ethan Zuckerman, "Intermediary Censorship," in *Access Controlled,* 71–84.

15. Miguel Helft and David Barboza, "Google Shuts China Site in Dispute Over Censorship," *New York Times*, March 22, 2010, http://www.nytimes.com/2010/03/23/technology/23google.html?_r=1.

16. Rebecca MacKinnon, "China's Censorship 2.0: How Companies Censor Bloggers," *First Monday* (February 2006), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2378/2089.

17. Wen Yunchao, "The Art of Censorship," *Index on Censorship* 39, no. 1 (2010): 53–57.

18. For detailed analysis of the Yahoo! China case, see Rebecca MacKinnon, "Shi Tao, Yahoo!, and the Lessons for Corporate Social Responsibility," working paper presented December 2007 at the International Conference on Information Technology and Social Responsibility, Chinese University, Hong Kong, http://rconversation.blogs.com/YahooShiTaoLessons.pdf.

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

20. MacKinnon, "Networked Authoritarianism in China and Beyond."

21. Kathrin Hille, "How China Polices the Internet," *Financial Times*, July 17, 2009, http://www.ft.com/cms/s/2/e716cfc6-71a1-11de-a821-00144feabdc0.html; David Bandurski, "China's Guerrilla War for the Web," *Far Eastern Economic Review*, July 2008, http://feer.wsj.com/essays/2008/august/chinas-guerrilla-war-for-the-web.

22. Congressional-Executive Commission on China, *2009 Annual Report*, http://www.cecc.gov/pages/annualRpt/annualRpt09/CECCannRpt2009.pdf.

23. "Chinese State Security Arrests, Indictments Doubled in 2008," *Dui Hua Human Rights Journal*, March 25, 2009, http://www.duihua.org/hrjournal/2009/03/chinese-state-security-arrests.html.

24. Information Office of the State Council of the People's Republic of China, *The Internet in China,* June 8, 2010, http://china.org.cn/government/whitepaper/node_7093508.htm.

25. David Talbot, "China: Our Internet Is Free Enough," *MIT Technology Review,* June 16, 2010, http://www.technologyreview.com/web/25592/page1/.

26. Please refer to the South Korea country profile in this volume for a comprehensive overview of South Korean laws and regulations aimed at controlling online speech.

27. International Telecommunication Union (ITU), "Internet Indicators: Subscribers, Users and Broadband Subscribers," 2009 figures, http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False.

28. Jonathan Watts, "World's First Internet President Logs On," *The Guardian*, February 24, 2003, http://www.guardian.co.uk/technology/2003/feb/24/newmedia.koreanews.

29. Elizabeth Woyke, "OhmyNews Chooses Influence over Income," *Forbes*, April 3, 2009, http://www.forbes.com/2009/04/02/internet-media-video-technology-korea-09-media.html.

30. Reporters Without Borders, "Enemies of the Internet, Countries under Surveillance," March 12, 2010, http://en.rsf.org/IMG/pdf/Internet_enemies.pdf.

31. Frank La Rue, "Full Text of the Press Statement Delivered by the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Mr. Frank La Rue, after the Conclusion of His Visit to the Republic of Korea," May 17, 2010, http://www2.ohchr.org/english/issues/opinion/docs/ROK-Pressstatement17052010.pdf.

32. Ibid.

33. Eric Fish, "Is Internet Censorship Compatible with Democracy? Legal Restrictions of Online Speech in South Korea," *Asia-Pacific Journal on Human Rights and the Law* 10, no. 2 (2009): 43–96.

34. Jonathan Krim, "Subway Fracas Escalates into Test of the Internet's Power to Shame," *Washington Post,* July 7, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/07/06/AR2005070601953.html.

35. "Korean Companies Still Open to Cyber Attacks," *Asia Times Online,* November 21, 2003, http://www.atimes.com/atimes/Korea/EK21Dg02.html.

36. "Cyber Bullying Campaign against Korean Singer Dies Down," Agence France-Presse, October 13, 2010, http://www.google.com/hostednews/afp/article/ALeqM5ig4StQI4mbvccWeFCGC5uuihUyAg?docId=CNG.9dd1a1176881e712993720a765eec626.1d1.

37. Joint Korean NGOs for the Official Visit of the Special Rapporteur to the Republic of Korea, *NGO Report on the Situation of Freedom of Opinion and Expression in the Republic of Korea since 2008*, April 2010, http://kctu.org/7978.

38. Byongil Oh, "Republic of Korea," *Global Information Society Watch 2009,* Association for Progressive Communications and Humanist Institute for Cooperation with Developing Countries, 150–152, www.apc.org/system/files/GISW2009Web_EN.pdf.

39. Ibid.

40. Matthias Schwartz, "The Troubles of Korea's Influential Economic Pundit," *Wired Magazine,* October 19, 2009, http://www.wired.com/magazine/2009/10/mf_minerva.

41. Song Jung-a, "S. Korean Court Rules on Internet Law," *Financial Times,* December 28, 2010, http://www.ft.com/cms/s/0/38b354a4-126d-11e0-b4c8-00144feabdc0.html.

42. Fish, "Is Internet Censorship Compatible with Democracy?"

43. Lee, Kwang-Suk, "Surveillant Institutional Eyes in Korea: From Discipline to a Digital Grid of Control," *The Information Society* 23, no. 2 (2007): 119–124.

44. Stephen Shankland, "YouTube Korea Squelches Uploads, Comments," *CNET,* April 13, 2009, http://news.cnet.com/8301-1023_3-10218419-93.html.

45. *The Hankyoreh*, "S. Korea May Clash with Google over Internet Regulation Differences," April 21, 2009, http://english.hani.co.kr/arti/english_edition/e_international/350252.html.

46. Kim Tong-hyung, "Google Avoids Regulations, Korean Portals Not So Lucky," *Korea Times,* April 27, 2009, http://www.koreatimes.co.kr/www/news/tech/tech_view.asp?newsIdx=43939&categoryCode=129.

47. Kim Tong-hyung, "Is Korea Turning into an Internet Police State?" *Korea Times*, April 9, 2009, http://www.koreatimes.co.kr/www/news/tech/2010/05/133_42877.html.

48. Please refer to the India country profile in this volume for a comprehensive overview of Indian laws and regulations aimed at controlling online speech.

49. International Telecommunication Union (ITU), "Internet Indicators: Subscribers, Users and Broadband Subscribers."

50. "India to Have 'Billion Plus' Mobile Users by 2015: Executive," *Economic Times,* November 18, 2009, http://economictimes.indiatimes.com/News/Economy/Finance/India-to-have-billion-plus-mobile-users-by-2015-executive/articleshow/5242284.cms; Shilpa Kannan, "India's 3G Licence Bidders Bank on Big Change," BBC News, April 7, 2010, http://news.bbc.co.uk/2/hi/business/8607866.stm.

51. Noah Schachtman, "How Gadgets Helped Mumbai Attackers," *Wired Magazine*, December 1, 2008, http://www.wired.com/dangerroom/2008/12/the-gagdets-of/.

52. Mehul Srivastava and James Rupert, "China-Linked Hackers Attacked India, Researchers Say," *Bloomberg Business Week*, April 6, 2010, http://www.businessweek.com/news/2010-04-06/researchers-find-china-linked-cyber-spy-ring-targeting-india.html; Information Warfare Monitor and the Shadowserver Foundation, *Shadows in the Cloud: An Investigation into Cyber Espionage 2.0*, April 6, 2010, http://www.shadows-in-the-cloud.net.

53. See the India country profile in this volume.

54. Nishant Shah, "Subject to Technology: Internet Pornography, Cyber-terrorism and the Indian State," *Inter-Asia Cultural Studies* 8, no. 3 (2007): 349–366.

55. Amol Sharma and Jessica Vascellaro, "Google and India Test the Limits of Liberty," *Wall Street Journal,* January 4, 2010, http://online.wsj.com/article/SB126239086161213013.html.

56. An annotated copy of the full text can be found at: http://cyberlaws.net/itamendments/IT%20ACT%20AMENDMENTS.PDF.

57. Sharma and Vascellaro, "Google and India Test the Limits."

58. "Govt Can't Ban Porn Websites for Obscenity," *Economic Times,* February 11, 2010, http://economictimes.indiatimes.com/infotech/internet/Govt-cant-ban-porn-websites-for-obscenity/articleshow/5558340.cms.

59. Sevanti Ninan, "In the Name of National Security," *The Hindu,* June 7, 2009, http://www.hindu.com/mag/2009/06/07/stories/2009060750090300.htm.

60. Vikas Bajaj, "India Warns It Will Block BlackBerry Traffic That It Can't Monitor," *New York Times,* August 12, 2010, http://www.nytimes.com/2010/08/13/technology/13rim.html.

61. Phred Dvorak, Amol Sharma, and Margaret Coker, "RIM Offered Security Fixes," *Wall Street Journal,* August 14, 2010, http://online.wsj.com/article/SB10001424052748703960004575427312899373090.html.

62. Andrew Vanacore, "BlackBerry CEO Suggests Route to Eavesdropping," *Associated Press*, September 27, 2010, http://www.msnbc.msn.com/id/39387290/ns/technology_and_science-security/.

63. "India Extends BlackBerry Access Deadline," Agence France-Presse, October 12, 2010, http://www.google.com/hostednews/afp/article/ALeqM5h9tMlmC3AyuCjurj2tA4rPZj0alg?docId=CNG.3af003c84a71aeca2db44ba857bb01cc.401.

64. Vikas Bajaj and Ian Austen, "India's Surveillance Plan Said to Deter Business," *New York Times*, September 27, 2010, http://www.nytimes.com/2010/09/28/business/global/28secure.html.

65. S. Ramadoral, "Don't Disconnect India," *Hindustan Times*, September 21, 2010, http://www.hindustantimes.com/News-Feed/columns/Don-t-disconnect-India/Article1-603075.aspx.

66. Google, "Google Transparency Report: Government Requests," http://www.google.com/transparencyreport/governmentrequests/.

67. Pavan Duggal, "Internet and Democracy in India: A Report," in *Rhetoric and Reality: The Internet Challenge for Democracy in Asia,* ed. Indrajit Banerjee (Singapore: Times Media Academic Publishing, 2003), 61–98.

68. Raman Jit Singh Chima, "The Regulation of the Internet with Relation to Speech and Expression by the Indian State," Social Science Research Network, April 25, 2008, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1237262.

69. Gurumurthy Kasinathan and Parminder Jeet Singh, "India," Global Information Society Watch 2009, Association for Progressive Communications and Humanist Institute for Cooperation with Developing Countries, 127–130, www.apc.org/system/files/GISW2009Web_EN.pdf.

70. "Edward Tian: Google Is China's Best Tool for Understanding the West," *China Digital Times,* April 15, 2010, http://chinadigitaltimes.net/2010/04/edward-tian-google-is-chinas-best-tool-for-understanding-the-west/.

71. See, for example, "China Not Alone in Internet Regulation," *China Daily*, December 3, 2009, http://www.chinadaily.com.cn/opinion/2009-12/03/content_9111690.htm.

72. Aron Cramer and Zachary Karabel, *Sustainable Excellence: The Future of Business in a Fast-Changing World* (New York: Rodale, 2010).

73. United Nations Human Rights Council, *Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development—Protect, Respect and Remedy: A Framework for Business and Human Rights*, April 7, 2008, http://www.reports-and-materials.org/Ruggie-report-7-Apr-2008.pdf.

74. Ibid.

75. Aron Cramer and Jeremy Prepscius, "Corporate Social Responsibility in Asia," *Global Asia* 2, no. 3 (Winter 2007), http://globalasia.org/new/l.php?c=e113.

76. Marc Newsona and Craig Deegan, "Global Expectations and Their Association with Corporate Social Disclosure Practices in Australia, Singapore, and South Korea," *International Journal of Accounting* 37 (2002): 183–213.

77. Subratesh Ghosh, "Trusteeship in Industry: Gandhiji's Dream and Contemporary Reality," *Indian Journal of Industrial Relations* 25, no. 1 (July 1989): 35–44.

78. Tata company, "About" page, http://www.tata.com/aboutus/articles/inside.aspx?artid=1U2QamAhqtA=.

79. Mahabir Narwal and Tejinder Sharma, "Perceptions of Corporate Social Responsibility in India: An Empirical Study," *Journal of Knowledge Globalization* 1, no. 1 (2008): 61–79.

80. Ibid.

81. Ki-Hoon Lee and Dongyoung Shin, "Consumers' Responses to CSR Activities: The Linkage between Increased Awareness and Purchase Intention," *Public Relations Review* 36, no. 2 (June 2010): 193–195.

82. Moon Chung-in and Lim Sung-hack, "Weaving through Paradoxes: Democratization, Globalization, and Environment Politics in South Korea," *East Asian Review* 15, no. 2 (Summer 2003): 43–70.

83. Ibid.

84. Cramer and Karabell, *Sustainable Excellence*, 82–83.

85. Ibid.

86. Wales et al., *Big Business, Big Responsibilities,* 119–124.

87. "New Responsibilities in the Networked Age," in Wales et al., *Big Business, Big Responsibilities*.

88. Cramer and Prepscius, "Corporate Social Responsibility in Asia"; Simon Powell and Jonathan Galligan, *Ethical Asia: Corporate Good Guys? It's All about Labour and Environment,* CLSA Asia-Pacific Markets, November 1, 2010, https://www.clsa.com/assets/files/reports/CLSA-Ethical-Asia.pdf.