Toward the New Sullivan Principles in the Information Age: Conflicts and Challenges of Multinational Information Technology Companies in Asian Countries

Byul Shin

Rensselaer Polytechnic Institute,
110 Eighth Street, Troy, New York 12180, USA
shinb2@rpi.edu

Abstract. A free and open communication environment is essential for a democratic society. Information and Communication Technologies (ICTs) serve as a basic structure for creating democratic communication environments. We have to try to understand ethical issues which ICTs can cause and the importance of multinational companies' social responsibility. This paper presents case studies in conflict between governments and multinational information technology (IT) companies over internet regulations in Asia, specifically in China and South Korea. By analyzing recent conflicts, we develop an improved understanding of the embedded values of information technology and its possible effects on society. This analysis also allows us to anticipate possible future problems and understand future information environments. Furthermore, I suggest basic ethical concepts, identifying six principles which multinational information technology companies should consider when they implement their technology in other countries.

1 Introduction: Internet Regulation and the Importance of Private Companies

Cyberspace has become not a free space anymore [1]. The online world is a place which is controlled by each country's government regulations using such means as filtering, censorship, and surveillance. Regulations continue to evolve, just as technologies do. Ronals Deibert and Rafal Rohozinski analyze and categorize three types of government regulation: first generation control, second generation control, and third generation control. First generation internet control techniques involve denying access to specific internet resources by directly "blocking access to servers, domains, keywords, and IP address" [2]. Second generation techniques involve the consolidation of legal and technical control over the online environment, allowing the country's government to take quick action in future problematic situations. Third generation techniques involve distributing pro-government information or information that discredits or demoralizes political opponents in order to lead public opinion in cyberspace. Governments, also, try to keep and use any data that will make trouble for political opponents [2].

P.L.P. Rau (Ed.): Internationalization, Design, HCII 2011, LNCS 6775, pp. 393–401, 2011.

IT companies play an important and specific role in this situation. IT companies have a better understanding than government or individuals about the technological structures and mechanisms of the information world. The companies need to have close relationships with both governments and individuals. They have to fulfill government requests, while serving their customers, who are both users and citizens. In many cases, regulative actions make the companies implement technology that can violate human rights, invade privacy, and limit freedom of speech. Sometimes, regulative actions conflict with a company's own values regarding the uses of technology. When this occurs, the companies have to make difficult choices among respecting the law by complying with government requests, protecting their own values and profits, or serving the rights and interests of their users. Another problem is that the situation and context of regulatory actions varies depending on the individual government. Since many major IT technology companies are multinational companies, this variety of contexts may represent an extraordinary challenge.

Each country's situation, internet-related regulations, and conflicts are different, but they can be comparatively considered in an international context. Asian countries, part of a huge economic boom, have become venues for these problems because of their highly varied government structures and regulations and because technology companies want access to their markets. Most major information technology companies would like to succeed in Asia. However, the complex differences between the social and cultural contexts in the region make it difficult, and place companies in some controversial situations.

Compared to western countries, Asian countries are culturally, socially, and politically diverse and different from the western countries in which most multinational companies originate. Also in many Asian countries, governments have traditionally intervened in private companies and industry, and have historically repressive traditions of media control [3][4]. Therefore, studying cases in the region offers us examples helpful in developing an understanding of current problems and conflicts and in anticipating the future of the internet environment.

2 Case 1. China vs Google

China has one of the highest levels of information control technology in the world [5]; the Chinese government intends to control all information that comes in and out of the country. The government has required all IT companies in the country to enforce a high level of censorship and surveillance and to provide dedicated IT experts and tools for these purposes. Multinational IT companies have also been ordered to follow these government requests and are asked to engage in self-censorship and to provide individuals' records without appropriate legal procedures, even though this is quite different from what they do in their home countries.

Google, the company that has the world's largest search engine, highly censored all information provided to its users in mainland China. For example, it did not allow access to some politically controversial information, such as information about the Tiananmen Square protests. However, the company decided not to follow the Chinese government's strong self-censorship requests, insisting that they limit free speech on the web [6].

In March of 2010, Google announced it would no longer censor information as the Chinese government had required, redirecting all online requests and traffic arriving at google.cn to its Hong Kong branch, google.com.hk., which provides uncensored search results.[1] The Chinese government showed concern about Google's decision, by warning the company it would not be able to get its Internet Content Provider (ICP) license renewed, an annual requirement. In response, Google stopped redirecting its traffic in early July. Instead, it made a landing page that allowed users to choose between Google China and Google Hong Kong. Finally, the Chinese government renewed the company's ICP license, though strong contentions between the government and the company continue. Also, some services of Google China temporarily remain blocked in mainland China, perhaps by the Chinese government – Google reports this outage is not due to a technical problem [7].

Keith B. Richburg says this conflict between Google and China is one between free speech online and strict censorship and control [8]. The issues which Google raised regarding its conflict with the Chinese government were mainly two: censorship and freedom of speech. As the company said in their official blog, "self-censorship is a non-negotiable legal requirement" in China [6]; monitoring published online material is an IT company's responsibility. Both ISPs and ICPs have to block, censor, and report whatever the government designates to be "illegal," generally socially sensitive issues or threats to national security [2]. Illegal content includes not only commonly regarded socially unacceptable contents, such as pornography and gambling, but also politically controversial information and Western media [9]. The extent of government-defined illegality is not only broad but also vague. For example, descriptions of banned content include such terms as "Western decadent culture" and "information with political implications" [10].

China is a highly censored country. Serious ethical problems in China, of which IT companies must be aware, include the possibility that technology will be used for violating human rights, including the freedoms of speech and access essential for democratic society. The self-censorship mandated for IT companies involves implementing access/administrative/personal control over individual and institutional computer systems, installing censorship software at each information point and at gateways to international networks, and retaining data [10][4]. The main external reason given by the government for internet regulation in China is social security, but in many cases censorship and filtering are likely used for political reasons to block anti-government information and unaccepted viewpoints such as those regarding illegal political activity. Censorship has been applied to web sites run by Tibetian exiles and the Taiwanese government [2] [10].

Information technology can be used to threaten individuals' safety as well as limit free communication. One of the reasons Google decided not to follow the Chinese government's regulation requests was that the company found that human rights activists' Gmail accounts had been hacked. The company's official blog announced that, "Gmail accounts of dozens of human rights activists connected with China were being routinely accessed by third parties" [6]. China has also been suspected of monitoring and data-mining its political opposition, journalists, and human rights activists' private information, such as personal email accounts and personal web

[1] http://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html

activity records. The information can be used for law enforcement, and used as evidence in individual arrests. It is clear that many political dissidents active in cyberspace in China have been arrested and harassed. Currently, it appears that at least 72 individuals are in prison in connection with information crimes [5]. These arrests and imprisonments occur without proper legal grounds or formal process in many cases.

3 Case 2. South Korea vs YouTube

South Korea is a democratic country [11]. The country provides higher levels of freedom of information and speech by comparison to China. Perhaps, as a result, the country's approach to internet regulation is based on a legal process, rather than simple rule by authority. As one of the most highly-connected countries in the world, South Korea was quick to develop social and governmental awareness about internet regulation. They were first to adopt new regulation methods, such as real name requirements, an approach on a national level [12]. However, there has been controversy around government efforts to have more control over the information world in recent years.

In April of 2009, after an amendment to the Information Act took effect, YouTube Korea decided to stop their uploading services in South Korea in essence refusing to follow the new version of the act. The amendment to the information act included the extension of real name registration requirements. Under these requirements, a website which has online content publishing features and more than 100,000 daily visitors has to confirm users' real names and resident registration numbers. Previously, the real name registration requirements were only applied to websites with 300,000 daily visitors or more [12].

Real name registration requirements have been actively discussed in South Korea. Assenters to the rule say that the rule is effective in reducing cyberviolence, including online bullying, abusive comments, and the spread of illegal content, as it makes users feel more responsible for their published contents and comments [13]. Opponents insist that the rule can violate such human rights as privacy and freedom of expression in cyberspace.

Anonymous internet communication has had positive effects on the creative development of internet culture in South Korea. It has encouraged more participation in online activity, critical opinions on culture and society, and equal and participatory relationships between citizens [14]. Specifically, anonymous communication on the internet has expanded political discourse. Although South Korea is a democratic republic, the level of media freedom is not high [15]. Social and political discussions in the country were long been repressed under dictatorial and military regimes until the 1990s, and political discourse among ordinary citizens was suppressed before the introduction of the internet. Because anonymous communication on the internet has played an important role in expanding political discourse and promoting citizen participation, it can be regarded as having more positive than negative effects on society.

Real name registration requirements could have negative effects. They raise personal information security and privacy issues, in that individuals' personal information would be shared by many private and public sectors, and most internet activities would be recorded and traceable. Real name registration requirements have the potential to limit individuals' free speech and could be used as a tool to strengthen government control and surveillance of ordinary people [16]. Besides this rule, the amendment of the Information Act contains many changes to reinforce government surveillance and repress individual freedoms. One of the most important changes imposes restrictions on defamatory information in cyberspace requiring portals to delete or suspend online articles if anyone complains an article is "fraudulent" or "slanderous" [2]. Though the Korean government claims that the amendment is only intended to keep the internet clean and orderly, this increased regulation is suspected to be a response to concerns about the internet's growing effect on political discourse and its power to mobilize people, as demonstrated in the massive civic protest in 2008 [17].

The conflict between YouTube and the Korean government has raised several issues regarding internet regulation in the country. First, it has reinvigorated the debate about the appropriateness of internet regulation. Even though the regulation was enacted by a legal process, an inherent ethical problem is embedded in even the most valuable information technology, because it can possibly be used to control and monitor individual lives, a point which Korean society may not have sufficiently considered. Second, the conflict has raised issues regarding the effectiveness of internet regulation, and the difficulty in predicting whether regulations have the desired consequences. Although YouTube announced it has closed upload services in South Korea, internet users in Korea can still use these services, including the upload service, freely if they switch their preference settings to another country.

This decision by YouTube has helped to raise social concerns, creating conditions in which internet users are frightened of that their communications might be monitored, limiting free speech rather than decreasing cyberviolence. Research shows that after the implementation of the law, the number of postings and users who write and reply significantly decreased, but the number of slanderous comments and swear words was not significantly reduced [18].

YouTube's reaction against the South Korean government is only possible because the company is multinational, hosted larger market outside of the country. Therefore, it is less restricted by local government. The YouTube case is meaningful, not only because it raises important questions about internet regulation and human rights in Korean society, but also because the company was the first to refuse to follow the law and can serve as an example to other IT companies. Note, though, that the option to refuse to comply may not be available or could be very difficult for domestic companies.

4 New Sullivan Principles for the Information Age

When an IT company starts to do business and implement its technology in other country, localization of its product is important. In most cases, the issue is how to design and implement appropriate technology in each local situation. However, IT companies also have to set up their policies and make business decisions based on each country's context including local laws, cultural and religious background, and social norms [19]. Localization may require companies to violate democratic principles.

ICTs are not just a tech product but also an important infrastructure. A flourishing information society and culture will come about when certain preconditions are met:

> (1) a functioning public sphere (print, electronic, digital, broadband) open to broad participation and deliberative engagement among major social groups; (2) a percentage of the public communications system capacity reserved for non-commercial exploitation in order to strengthen the foundations of civil society and associational development; (3) guarantees of citizens' information rights through freedom of information laws, government transparency, and public service obligations for information providers to serve the public-opinion formation process; and (4) access to knowledge, information and an educational system that cultivates independent judgment instead of rote learning [3].

IT companies have to consider social responsibility when selling their technology. Technology is not neutral [20]. IT technology, specifically, has embedded value as a means of control and surveillance in society. People who deal in IT technology should be cautious that their technology is not used to repress society.

Multinational IT companies, especially, have to aware of the ethical issues of their technology when they implement it in another country. Since their technology is often hosted outside of the country they are seeking entry to, these companies are less influenced by local laws. It is easier for a multinational company to raise an objection to a local law than for a local company. They can better consider ethical values and compare the local situation to that in their home countries or in other countries in where they do business. Their reaction for or against government can serve as an example and possibly influence local companies. Furthermore, in the long term, their actions can cause future policy changes in local governments, perhaps leading to the alleviation of regulations and controls [9].

The Sullivan Principles were a code of conduct that was developed by the African-American preacher Rev. Leon Sullivan, in 1977 for doing businesses in South Africa under apartheid. It was a set of ethical guidelines for multinational corporations to use in making decisions in an ethical way to protect the human rights of black workers in South Africa. It promoted corporate social responsibility and suggested values that corporations should think about when they operated their businesses in South Africa. The principles contained articles urging corporate awareness to local people in vulnerable situations, respect for universal human rights, the equal treatment of people both from their native countries and in the local country, and the improvement of social and living conditions of local people [21].

Many IT companies are not aware that ICTs are crucial to foster democratic environments in modern society. Also, some IT companies sell their technologies to governments even though they know those technologies are used to violate human rights and threaten human safety, and even though they have a social responsibility for the societies in which they run businesses [22].

Internet regulation is typically both positive and negative in its effects. It is needed to keep cyberspace secure, specifically to protect children and prevent cybercrime. However, as we've seen in the previous section, it can have harmful effects that can threaten individuals' freedom and rights. Ethical IT companies have to consider the potential for negative effects associated with the introduction of their technologies.

In the previous section, I explained possible ethical problems regarding ICTs and regulation by analyzing two cases, the conflict between Google and the Chinese government, and between YouTube and the South Korean government. Based on that analysis and using the original Sullivan Principles as a framework, I have developed six, specific ethical principles for multinational IT companies to think about when they implement their technology in other countries, to protect basic human rights and to foster democracy on the internet.

Principle #1: Multinational IT companies have to be aware that *users in local countries must be treated and respected the same as users in those companies' native countries.* This requires a guarantee of the same level of basic human rights for local users who use the companies' technologies and services.

Principle #2: When multinational IT companies receive legal regulation requests, they must consider whether *the regulation request is based on appropriate legal grounds and takes place in the context of a transparent legal procedure*.

Principle #3: *Multinational IT companies should avoid politically motivated internet regulations*, specifically those regulations imposed to enforce or exclude certain political ideologies, suppress political mobilization, or repress political dissidents or human rights activists.

Principle #4: Multinational IT companies must *provide free speech and free access to information for local users*. This doesn't mean they must provide unlimited freedom; companies have to respect local laws. But if they find that local laws significantly curtail freedoms and create highly restricted environments, then the companies should take appropriate ethical positions on the issues or laws.

Principle #5: Multinational IT companies have to *protect their users' personal security, private information, and identities*. Though companies might record and retain users' private information for technical reasons or customer services, they should not allow an individual's private information to be used either commercially or politically without that individual's consent.

Principle #6: Multinational IT companies must make an effort to *improve the overall information environments of local countries to foster a more democratic cyberspace*. A free and active communication environment is essential to the emergence of a democratic society. Multinational IT companies bear a social responsibility for their technologies' uses, and are partners in designing the overall social communication environment.

5 Conclusion

The recent increase in internet regulation creates conflicts between governments, IT companies, and citizens. In this paper, I focused on conflicts between governments and multinational IT companies. Since ICTs are relatively new, we do not have enough precedents for its regulation, and it is difficult to foresee the possible effects or problems associated with present and future regulation. Therefore, I analyzed two different cases: China vs. Google and South Korea vs. YouTube. Recent government internet regulations in those countries involve censorship, filtering, and surveillance which multinational IT companies are required to enforce potentially threaten basic human rights and individuals safety.

IT companies have to make difficult decisions, choosing between governments and users. I suggested basic principles to help multinational IT companies make ethical decisions based on these case studies and the framework of the Sullivan Principles. My new Sullivan Principles for the Information Age are designed to promote multinational companies' social responsibility, encourage more democratic societies and help the companies find an ethical balance between government requests and the protection of user rights and safeties, especially for companies that do business in other countries.

References

1. Margolis, M., Resnick, D.: Politics as Usual: the Cyberspace Revolution. Sage, Thousand Oaks (2000)
2. Deibert, R.: OpenNet Initiative: Access Controlled: the Shaping of Power, Rights, and Rule in Cyberspace. MIT Press, Cambridge (2010)
3. Venturelli, S.: Inventing E-regulation in the US, EU and East Asia: Conflicting Social Visions of the Information Society* 1. Telematics and Informatics 19, 69–90 (2002)
4. Gomez, J.: Dumbing Down Democracy: Trends in Internet Regulation, Surveillance and Control in Asia (2004)
5. Beiser, V.: The Curt Knock on the Door (2010)
6. Drummond, D.: A New Approach to China: an update, http://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html
7. Google Q&A Page Blocked in China (2010), http://www.chinaeconomicreview.com/dailybriefing/2010_08_04/Google_QandA_page_blocked_in_China.html
8. Google Compromise Pays off with Renewal of License in China, http://www.washingtonpost.com/wp-dyn/content/article/2010/07/09/AR2010070902137.html
9. Harwit, E., Clark, D.: Shaping the Internet in China: Evolution of Political Control over Network Infrastructure and Content. Asian Survey 41, 377–408 (2001)
10. Wang, G.: Regulating Network Communication in Asia: a Different Balancing act?* 1. Telecommunications Policy 23, 277–287 (1999)
11. Democracy Index, Economist Intelligence Unit (2010)
12. Google Refuses South Korean Government's Real-name System, http://english.hani.co.kr/arti/english_edition/e_international/349076.html
13. Hwang, C.: A Legal Study on the Anti-Cyberviolence on the Internet. Korea Communications Commission (2009) , 인터넷상 욕설, 악플 등 사이버 폭력 해소를 위한 법제도 개선방안 연구

14. Son S., Kim, S., Kim, H.: An analysis of Internet and Communication Policy in Korea based on Postmodern Theories. Korea Information Society Development Institute (2009) , 최근 통신정책 이슈에 대한 탈근대론적 재조명
15. World Press Freedom Index 2009 - The rankings. Reporters without Borders (2009)

. . . Baek, I.: The Policy Study on Protecting Freedom of Speech in the Internet. The National Human Rights Commission of the Republic of Korea (2004) ,. 인터넷에서의 표현의 자유 보호를 위한 정책 연구 보고서.

17. Kim, H.: Will Minerva Case Make ’Internet Regulation’ Salient (2009), http://www.zdnet.co.kr/news/news_view.asp?artice_id=20090421161359&type=det, 미네르바, '인터넷 규제정책' 도마에 올리나
18. Woo, J., Na, H., Choi, J.: An Empirical Analysis of the Effect of the Real-Name System on Internet Bulletin Boards: How the Real-Name System and User Characteristics Influence the Use of Slanderous Comments and Swear Words. Seoul National University 48, 71–96 (2010), 인터넷 게시판 실명제의 효과에 대한 실증 연구: 제한적본인확인제 시행에 따른 게시판 내 글쓰기 행위 및 비방과 욕설의 변화를 중심으로
19. Aykin, N.: Usability And Internationalization of Information Technology. CRC, Boca Raton (2005)
20. Deibert, R.: Access Denied: The Practice and Policy of Global Internet Filtering. The MIT Press, Cambridge (2008)
21. Sethi, S.P., Williams, O.F.: Creating and Implementing Global Codes of Conduct: An Assessment of the Sullivan Principles as a Role Model for Developing International Codes of Conduct—Lessons Learned and Unlearned. Business and Society Review 105, 169–200 (2000)
22. Seven “Corporations of Interest” in Selling Surveillance Tools to China | Electronic Frontier Foundation, http://www.eff.org/deeplinks/2010/01/selling-china-surveillance