The Information Society, 24: 40–46, 2008
Copyright © Taylor & Francis Group, LLC
ISSN: 0197-2243 print / 1087-6537 online
DOI: 10.1080/01972240701774774

Routledge
Taylor & Francis Group

PERSPECTIVE

Global Freedom of Expression Within Nontextual Frameworks

Johnny Hartz Søraker

Department of Philosophy, University of Twente, Enschede, The Netherlands

The increasing use of frameworks within which Internet users can contribute nontextual information constitutes a serious obstacle to government attempts to accurately censor and monitor Internet traffic. This development, as seen in the explosive growth of frameworks such as Second Life, YouTube, and Wikipedia, could lead to a transfer of regulatory power away from heavily regulated Internet Service Providers in nondemocratic regimes, into the hands of intermediaries that are more likely to uphold freedom of expression. Thereby, a development toward increasingly *enframed* and *nontextual* information can promote freedom of expression even in traditionally nondemocratic regimes. I analyze this development with regard to its possible implications for freedom of expression, online crime, and the role of private companies in international politics.

Keywords censorship, deliberative democracy, globalization, Internet governance, online crime, regulation, user-generated content, Web 2.0

In its early days, the Internet was often hailed as a promoter of global democracy insofar as it allowed previously oppressed minorities to voice their opinions and retrieve information without fear of persecution. The Web seemed like a perfect vehicle for promoting the fundamental ideals of deliberative democracy.[1] However, nondemocratic regimes, keen on reaping the economic benefits of the Internet, were quick to implement countermeasures to censor unwanted information and trace the identity of Internet users. Their primary means of doing so has been strict control over local Internet service providers (ISPs).

Consequently, one way of promoting freedom of expression worldwide lies in reducing the power of ISPs to regulate, and to transfer this power exclusively to Internet intermediaries that are subject to liberal democratic legal regimes. It could be argued, normatively, that certain aspects of the Internet ought to be centralized in order to bring this about.[2] The purpose of this article, however, is to consider and evaluate some recent trends on the Web that could contribute toward weakening the power of ISPs and local authorities, and to analyze how this might promote freedom of expression worldwide. Thus, allow me to emphasize that I leave it an open question whether global freedom of expression *ought* to be promoted and, even if so, whether it ought to be promoted in this manner.

THE ROLE OF INTERNET SERVICE PROVIDERS IN INTERNET REGULATION

Media censorship can be targeted at sources, targets, or intermediaries. On the Internet, sources (e.g., web sites) often reside outside governments' legal jurisdiction, and Internet users utilize such a wide range of software and hardware that regulation of targets becomes technologically impractical (cf. Goldsmith & Wu, 2006, pp. 67–73). Thus, the most convenient way to regulate the Internet is by targeting intermediaries. It is a common misconception that the Internet does not rely on specific intermediaries, that it "interprets censorship as damage and routes around it," and that local regulation of the Internet is impossible. However, one of the key elements of the Internet architecture is the Internet service provider (ISP), which is a necessary intermediary to access the Internet for most

Received 6 August 2007; accepted 4 October 2007.

I am indebted to Kristian Skagen Ekeli for substantial contributions to an earlier version of this article. I would also like to thank Philip Brey, Adam Briggle, Edward Spence, and an anonymous referee for their valuable feedback.

Address correspondence to Johnny Hartz Søraker, Department of Philosophy, University of Twente, Postbus 217, 7500AE Enschede, The Netherlands. E-mail: j.h.soraker@utwente.nl; web site http://www.utwente.nl/ceptes/research_staff/Soraker

users. Furthermore, Internet service providers are to some degree geographically fixed. That is, in order to facilitate a connection between the user's location and the Internet, the providers must necessarily be local and consequently abide by the rules and regulations in that regime.

All the information that ordinary Internet users send and retrieve is mediated by their ISP, which means that ISPs can—and usually do—keep detailed records of customers' Internet traffic. They can also implement mechanisms for filtering or monitoring certain kinds of information. Thus, ISPs constitute the most convenient "point of entry" for government authorities that seek to censor and/or monitor their citizens' Internet traffic. In most democratic regimes, ISPs have strict rules for how to use and store data about their users and typically do not release this information to third parties, including law enforcement agencies, unless presented with a court order. However, in some countries, ISPs are controlled by the government to such a degree that they can implement surveillance and filtering as they see fit. Consequently, the power of ISPs to filter and monitor the traffic of their users constitutes the biggest obstacle to providing equal freedom of expression worldwide. If we want to reduce the ability of governments to implement local regulations, culture-imperialist objections aside, one viable option is to reduce the power of ISPs. Interestingly, this could be the consequence of current trends on the Web.

Among the regulatory options available to ISPs, the most common methods are to block information that originates from specific sources or information that contains specific keywords. Typically, a list of blacklisted sources is compiled on the basis of one or more particular instances of information from a given web site, as in China's blocking of bbc.co.uk, or on the basis of a web site's general theme, as in China's blocking of playboy.com. A list of blacklisted keywords is usually compiled on the basis of whether it is likely to signify offensive content. Until recently, both methods have worked reasonably well from a regulator's point of view. However, I will argue that as the Web starts moving toward more dynamic, collaborative, and nontextual means of information transfer, these methods become increasingly inaccurate, overinclusive, and undesirable.

THE UNTRACEABILITY AND TRACEABILITY PROBLEMS

To get a clearer understanding of the relation between ISPs and their users' ability to express themselves freely and their ability to engage in online crime, we can distinguish between two problems, which I will refer to as *the traceability problem* and *the untraceability problem*.

1. *The traceability problem:* In virtue of assigning users' identification numbers (IP addresses) and mediating their Internet traffic, Internet service providers can easily implement mechanisms that censor and monitor information that contains blacklisted keywords or that is retrieved from blacklisted sources. Moreover, they can easily trace such activity to (nonsavvy) customers' real-life identities. Thus, the present Internet architecture implies that individual governments can censor and monitor their citizens' Internet use by exercising control over local Internet service providers. This is, for instance, the case in Burma, China, Iran, and Libya (cf. Reporters without Borders, 2006, pp. 106–134). As a result, anonymity is largely illusory in the countries where it is most needed, that is, countries in which the government keeps a tight grip on the media in general. Thus, the claim that the Internet is an entirely new medium that provides anonymity and democratic potential unparalleled by other media is vastly overstated. Instead, anonymity online is enjoyed mainly by citizens in countries where freedom of expression is already respected and constitutionally protected.
2. *The untraceability problem:* There is one group of people who can enjoy anonymity on the Internet, regardless of which country they reside in: the so-called "savvy users" (Ess, 2005, p. 103ff). It *is* possible to be completely untraceable on the Internet, but this is reserved for users with advanced knowledge of technology and "anonymizer tools." The majority of Internet users are not aware of how this works, but those who are determined enough can obtain the necessary tools and knowledge. These users can exploit this untraceability for all sorts of criminal purposes, including diffusion of child pornography, identity theft, and large-scale piracy.

It is this twofold problem that gives rise to the perception that freedom of expression and crime prevention online are mutually exclusive endeavors. One way to deal with the traceability problem, and to some degree the untraceability problem (as I will return to), would be to transfer regulatory power away from intermediaries that are geographically fixed and required to comply with local regulations. In other words, a first step would be to reduce the power of local ISPs.

There are numerous ways in which ISPs can be left in the dark. As mentioned, "savvy users" with advanced knowledge of the Internet technology can avoid censorship. Thus, one way of improving users' freedom of expression in nondemocratic regimes would be to educate users on how to use these technologies. This is a bit of a catch-22, however, since information on how to bypass censorship can also be easily censored. Moreover, one must be aware of the problem in the first place, or perceive it as such, in order to actively look for anticensorship tools and information. Thus, a better solution would be to keep

ISPs in the dark by default, with little or no need for the users themselves to understand the technological underpinnings. It can be argued that certain aspects of the Internet technology ought to be centralized in order to bring this about, but given the recent development toward what I will refer to as *enframed* and *nontextual* user-generated content, this might happen of its own accord.

ENFRAMED AND NONTEXTUAL INFORMATION

There has been much hype recently over what has been referred to as "Web 2.0," "Web 3.0," "Web 3.d," and the like. This development is for instance what prompted *Time Magazine* to name "You" as their person of the year in 2006 (Grossman, 2006). Although these labels are contested, they signify a development away from static, one-to-many, text-dominated web sites, toward dynamic, many-to-many frameworks that utilize nontextual elements to a larger degree. This can most clearly be seen in the explosive growth of various frameworks in which the users themselves provide the content. Examples include Wikipedia, MySpace, YouTube, Facebook, Second Life, and various blog service providers. This development has two implications that could seriously undermine current government regulations. I refer to this development as a move toward *enframed* and *nontextual* information.

Enframed Information

User-generated content increasingly takes place within preestablished frameworks such as Wikipedia, Facebook, or blog providers. This means that the source of a particular piece of information within such a framework, from an ISP's perspective, is the framework itself. In other words, a particular piece of information within such a framework cannot be singled out and censored on the basis of source (IP address), because this particular piece of information comes with the same source-address as every other piece of information from within the same framework. Thus, a regulator operating at the ISP level cannot censor a single article within, e.g., Wikipedia, but is left with a choice between censoring and allowing the framework as a whole.

As long as these frameworks are primarily textual, regulators can still resort to keyword censorship, however.[3] Thus, what I refer to as the enframing of user-generated content only creates an obstacle to censorship on the basis of blacklisted *sources*—which brings us to the next feature.

Nontextual Information

As mentioned, enframing information within large frameworks, where only a minor fraction of the content is deemed offensive, constitutes a problem with regard to source censorship. Yet keyword censorship is still an option. The reason why this method is still feasible is that text encoded as a digital representation can be decoded with relative ease. This is not the case, however, with nontextual information such as images, audio, and video. Information containing a given text string can easily be intercepted by an ISP, whereas information consisting of an image, pod cast, video, or three-dimensional (3D) model cannot. One reason is that it is clearly more difficult to decode nontextual information from a stream of data.[4] A more inherent problem is that information on the Internet is usually not transferred as a continuous stream of data, but as a series of fragmented packets that are normally assembled only on the receiving end. Although these packets are relatively small, they can contain a lot of textual information, since text typically requires only one or two bytes per character. Various forms of nontextual information, however, require large strings of data. Since these data are fragmented into small packets when transferred on the Internet, often traveling through different network nodes, any given packet only contains a fraction of an image, video, or something similar—a fraction that is meaningless in itself. To make matters even more difficult, there are countless different formats for representation and compression of nontextual information. Thus, the fragmented and diverse nature of nontextual information transfer on the Internet makes it nearly impossible to automatically determine its semantic contents.

It should be noted that censorship technology is of course becoming increasingly advanced in order to cope with these problems. With recent advances in deep packet inspection and automated pattern recognition, is it not just a matter of time before regulators can accurately censor specific pieces of information even if they are enframed and nontextual? Deep packet inspection (DPI) is a rapidly evolving technology, which has become popular mainly because it enables ISPs to cope with excessive use of bandwidth caused by file sharing. DPI works by inspecting the contents of a packet—or a flow of packets, known as deep flow inspection—and information can be censored based on whether or not there is a significant match between the content of the intercepted packet(s) and a library of blacklisted patterns. Currently, such libraries typically consist of signatures associated with specific applications, such as file-sharing applications. In other words, DPI does not disclose the content of the information, merely what type it is (cf. Anderson, 2007).

The problem is that even this rudimentary form of inspection has already led to concerns over significant reductions in information transfer speed. Thus, the crucial question becomes: Is it possible to automatically discern the semantic content of nontextual information without thereby dramatically reducing the speed of information transfer? Although pattern recognition is becoming more efficient and reliable, it is important to keep in mind that existing systems are primarily designed to recognize specific kinds of information, for instance a face or a license plate. When we take into consideration the seemingly infinite ways in which one can express oneself in a virtual environment such as Second Life, I think it is a fair bet that no foreseeable technology will be able to reliably disclose the semantic content of nontextual information, let alone so efficiently that it does not drastically reduce the speed of information transfer.

Taken together, this entails that particular content distributed via services such as YouTube, MySpace, and Second Life—being both nontextual and enframed—is nearly impossible to censor individually on the basis of both blacklisted keywords and sources. It also entails that the ISP can only detect that a user is exchanging information with a given framework and not the content of that information.[5]

To a higher degree than merely enframed content, where keyword censorship is still an option, censorship of nontextual, enframed content requires an all-or-nothing approach; *the framework in which nontextual, user-generated content is enframed must be accepted or rejected in its entirety*. This is evidenced by numerous recent examples of governments choosing "nothing." A Brazilian court recently ordered local ISPs to block access to the entire YouTube framework because of one video, and Pakistan decided to block the entire blogger.com framework in order to deal with a handful of blogs showing the controversial Muhammad cartoons (Beam, 2007).

MAKING THE ALL-OR-NOTHING CHOICE DIFFICULT

When Internet traffic becomes increasingly enframed and nontextual, regulators can no longer censor specific pieces of information. It is still possible to censor frameworks in their entirety, however. Why, then, is the developing situation different from the way regulations have been carried out in the past? After all, censoring sites like those of the *New York Times* and BBC generate instances of censoring entire frameworks because of a tiny fraction of unwanted information within those frameworks. What could make the all-or-nothing choice more difficult? There are three distinguishing characteristics of these developing frameworks that might convince regulators that the positive effects outweigh the negative.[6]

Virtual Economies as Real Economic Incentives

It might seem strange that some authorities use a lot of resources on censoring and filtering the Internet when it is in fact easier for governments to deny access completely.[7] The reason is of course that, despite the unwanted elements, the Internet provides a number of benefits that authorities would like to reap. The major incentive in this regard is of course economic. Do these nontextual frameworks provide any interesting economic incentives?

The proclaimed first virtual millionaire, Anshe Chung, hails from China. By selling virtual property in Second Life, Chung has acquired wealth that is estimated at a value of more than US$1 million. Relative to the level of income in China this is a staggering amount, which points to a very important characteristic of virtual economies. Although earning US$2000 per year in Second Life, by no means an extraordinary achievement, can constitute an interesting side income for Western citizens, it can actually constitute a livelihood in itself in countries with very low per capita income. Thus, a virtual environment such as Second Life, even at this early stage of development, can be seen as having major economic benefits. As more and more users find a way to make a living and more and more businesses find niches within nontextual frameworks, it becomes increasingly undesirable to deny access to these frameworks.

Nontextual Frameworks and the Future Internet

Although one should be careful with speculations about the future of technology, it seems reasonable to assume that more and more information will be retrieved from within giant frameworks, and more and more of this information will be nontextual. This development is of course correlated with the increasing use of broadband connections, which enables ordinary users to quickly and reliably transfer large amounts of data. Other indicators include the increasing number of organizations that already offer their services within virtual environments such as Second Life, including banks, embassies, and entertainment providers. Furthermore, Linden Labs, the creator of Second Life, recently released its client source code, a move that is strongly reminiscent of NCSA's decision to release the source code of its Mosaic browser back in 1993—by many described as the beginning of the Web as we know it. There are also numerous commercial and open source frameworks for nontextual, user-generated content currently being developed.[8] If more and more information and services will be made available in nontextual frameworks only, denying access to these frameworks in their entirety will prohibit not only an economically interesting venue, but also what might become one of the most significant portions of the Internet.

Crime Prevention Within Nontextual Frameworks

A final advantage to enframed content is that it provides a way of dealing with the aforementioned untraceability problem. In order to make any substantial harm in many of these nontextual environments, you need to verify your real-life identity. For instance, in Second Life, large-scale diffusion of illicit material is almost impossible without owning land, which requires you to be a paying customer, which in turn means that you need to provide your credit-card details. In the multiplayer, online game World of Warcraft you are unable to participate at all without using a credit card. Although using a credit card is not a foolproof way of being traceable, it is much more difficult to fake than an IP address. Thus, if a framework provider with these restrictions in place discovers a violation within its framework, it can not only ban that user but also, in serious cases, can provide accurate information about the user's real-life identity to the appropriate law enforcement agency.[9] Although problems regarding fraud and crime will not disappear, these frameworks will in many cases be able to accurately trace the identity of users engaging in serious online crime.

But if it is the case that criminals can more easily be traced within such frameworks, cannot nondemocratic regimes simply set up their own frameworks? For instance, governments can simply ban frameworks that do not comply with their laws and set up their own alternatives with these regulations in place. We have seen, however, that overly regulated frameworks do not lend themselves to the kind of creativity and entrepreneurship that is required in order to make these frameworks attractive. Thus, heavily regulated frameworks are unlikely to provide the same kind of benefits. Indeed, when frameworks have become too heavily policed, the result has been that users have abandoned it, and often mass migrated toward alternative, more liberal frameworks. This is, for instance, what happened to the Sims Online, where many of its previous inhabitants moved to Second Life. Due to recent events, we can witness similar responses to Second Life and YouTube.[10]

In summary, if these nontextual frameworks come to have significant economic benefits, to constitute a significant portion of the Internet and to be better equipped to deal with serious crime internally, then the previously mentioned all-or-nothing choice will become a difficult one. Thereby, nontextual environments can be seen as promoting global freedom of expression, given (1) that user-created content enframed in nontextual environments cannot be censored or filtered on a case-by-case basis, thereby leaving authorities with an all-or-nothing choice, and (2) that these frameworks become sufficiently beneficial so as to make it undesirable to censor them in their entirety. If this holds, local regulations become vastly more difficult and the Internet might come to realize its full potential as a truly democratic and global venue in which communication and information can be freely exchanged across borders—within nontextual frameworks.

NONTEXTUAL FRAMEWORK PROVIDERS AND INTERNATIONAL POLITICS

So far I have portrayed a somewhat optimistic account of these nontextual frameworks and how they might foster global freedom of expression, but there are of course some important problems related to this development. One technical problem is that many of these frameworks will require broadband and use of credit card, which could be seen as a digital divide that often runs along the same lines as that between democratic and nondemocratic regimes. This is not necessarily the case, however, as evidenced by the fact that China has the highest number of broadband users in the world.

Another legitimate concern is that these providers could take the easy way out and comply with any official request to remove unwanted material; we have seen numerous examples of intermediaries such as Google, YouTube, and Skype giving in to dictatorship requirements.[11] As long as there is competition between providers, however, it is to be expected that customers will drive providers toward liberal democratic policies. Furthermore, competition between providers of nontextual frameworks will of course be international. Based on the short history of framework providers and Internet users' preferences, it is reasonable to assume that the survivors will be the providers that do not regulate excessively—regardless of which regime they reside in. Indeed, the freedom to choose between framework providers with differing regulations is what distinguishes these intermediaries from geographically fixed Internet service providers, and the reason why transferral of power away from the latter might promote global freedom of expression online.[12]

A more dramatic scenario could be that the transferral of regulatory power away from authorities and into the hands of private companies can give rise to highly tense and complex international relations, with framework providers finding themselves in the midst of international politics. For instance, if foreign authorities—that is, authorities with no legislative power over the providers of the nontextual framework in question—would like to allow access to a framework but rid it of certain unwanted elements, then they would have to direct this concern to the framework providers and hope that they will comply. Foreign authorities do not have the means to directly threaten the providers if they do not comply, but they can instead threaten the authorities to which the providers ultimately must answer. This could lead to scenarios in which foreign authorities threaten, e.g., U.S. authorities (by diplomatic or other means) to have them force the framework providers into complying with the request. Within U.S. jurisdiction there is of course little U.S. authorities can do as long as the content within the framework falls within freedom of speech and does not violate U.S. law. However, if the stakes are high enough, which they often are in international politics, authorities might threaten the providers on the basis of some kind of technicality or by means of the mere threat of legal sanctions. The outlined development can, in other words, place these providers in the middle of international politics to an even higher degree than today.

CONCLUSION

The way in which framework providers might find themselves in the middle of international politics should remind us to be aware of the power of private companies at the expense of authorities. From the perspective of deliberative democracy, it is to be hoped that users will drive providers to remove content only in cases of clearly illicit material, such as diffusion of child pornography. There will obviously be problems with this development, both foreseen and unforeseen. However, increased use of nontextual frameworks with user-generated content and obvious benefits to any government can compel nondemocratic regimes to allow venues where users from all over the world can meet on equal terms, free from the actual and panoptical consequences of being subject to authorities that severely restrict freedom of expression online.

NOTES

1. The scope of this article does not allow for a detailed discussion of the ideas and ideals of deliberative democracy, but one of its cornerstones is that "decisions should be made as a result of a thorough and reasoned discussion in order to improve the basis of information and enhance the level of reflection among the participants" (Ekeli, 2005, p. 433). For the recent revival of theories of deliberative democracy, see, e.g., Elster (1986), Dryzek (1990), Rawls (1993), and Habermas (1996).

2. See, e.g., Søraker, 2006b.

3. This is reflected in the fact that China on numerous occasions has blocked the entire Wikipedia, but in periods in which it has been allowed, whether or not a particular article is censored is based on the textual content. See for instance http://yro.slashdot.org/comments.pl?sid=200323&cid=16403351 for an example of how the article on the Tiananmen protests was blocked, whereas the article on Tienamen (slightly alternate spelling) remained accessible.

4. This can be seen in web sites that utilize so-called CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart), i.e., grained or distorted images whose content cannot be made out by a computer. The difficulty of automatically discerning the content of images by way of pattern recognition is also exploited by spammers, who often use images instead of text in their e-mails to bypass spam filters (cf. http://en.wikipedia.org/wiki/Captcha and http://en.wikipedia.org/wiki/Image_spam).

5. It should be noted that nontextual, enframed information *can* be intercepted if it is identified by metadata, i.e., textual information describing what the video, image or audio is about. Many companies run scripts that are designed to find copyrighted material posted to video sharing sites, but this is difficult for two reasons. First, in order to remove the material in question they rely on the cooperation of the framework providers (I return to this point later). Second, users who post copyrighted material often find ways of altering metadata so as to make it difficult to search for, yet easily recognizable for users, for instance when labeling the movie Shrek as $hr3k.

6. These positive characteristics can be described as the basis of *pragmatic* arguments, in contrast with arguments based on ethical theories or political ideologies, which often do not lend themselves to cross-cultural argumentation (cf. Søraker, 2006a).

7. Denying Internet access to its citizens, save a select few, has for instance been the strategy of North Korea.

8. Among the most interesting are Sony's *Home* for their PS3 console, the Chinese *HiPiHi* and the Open Source project *OpenSim.*

9. For instance, the real-life identity of a Second Life avatar was recently disclosed following a copyright lawsuit (http:// secondlife.reuters. com/stories/2007/07/20/paypal-hands-over-john-doe-information/).

10. See, e.g., Second Life Herald's "Sim Movie Commemorates TSO Diaspora" (http://www.secondlifeherald.com/slh/2004/05/sim_movie_comme.html) and "The Disneyification of the Second Life" (http://www.secondlifeherald.com/slh/2007/07/the-disneyifica.html).

11. See Reporters Without Borders' "Dictatorships get to grips with Web 2.0," http://www.rsf.org/article.php3?id_article=20839.

12. A very interesting development in this regard is what will happen now that Linden Lab has banned gambling in Second Life due to U.S. gambling regulations. It will be interesting to note how U.S. authorities will deal with the advent of framework providers residing in countries where gambling is legal.

REFERENCES

Anderson, Nate. 2007. Deep packet inspection meets 'Net neutrality, CALEA. *Ars Technica,* July 25, 2007, http://arstechnica.com/articles/culture/Deep-packet-inspection-meets-net-neutrality.ars (accessed September 10, 2007).

Beam, Christopher. 2007. Can Brazil ban Youtube? How countries censor the Internet. *Slate,* January 10, 2007, http://www.slate.com/id/2157399/ (accessed July 1, 2007).

Brey, Philip. 1999. The ethics of representation and action in virtual reality. *Ethics and Information Technology* 1(1):5–14.

Dryzek, John. 1990. *Discursive democracy. Politics, policy, and political science.* Cambridge: Cambridge University Press.

Ekeli, Kristian Skagen. 2005. Giving a voice to posterity—Deliberative democracy and representation of future people. *Journal of Agricultural and Environmental Ethics* 18(5):429–450.

Elster, Jon. 1986. The market and the forum: Three varieties of political theory. In *Foundations of social choice theory,* eds. J. Elster and A. Hylland, pp. 103–132. Cambridge: Cambridge University Press.

Ess, Charles. 2005. Being in place out of place/Being out of place in place. In *Technology in a global and multicultural society*, eds. M. Thorseth, and C. Ess, pp. 91–114. Trondheim: NTNU University Press.

Goldsmith, Jack, and Wu, Tim. 2006. *Who controls the Internet?* Oxford: Oxford University Press.

Grossman, Lev. 2006. Time's person of the year: You. *Time Magazine*, December.

Habermas, Jürgen. 1996. *Between facts and norms*. Cambridge, MA: MIT Press.

Rawls, John. 1993. *Political liberalism*. New York: Colombia University Press.

Reporters Without Borders. 2003. *The Internet under surveillance—2003 Report*. http://www.rsf.org/IMG/pdf/doc—2236.pdf (accessed July 10, 2007).

Reporters Without Borders. 2006. *Freedom of the press worldwide in 2006*. http://www.rsf.org/IMG/pdf/report.pdf (accessed July 18, 2007).

Søraker, Johnny Hartz. 2006a. The role of pragmatic arguments in computer ethics. *Ethics and Information Technology* 8(3):121–130.

Søraker, Johnny Hartz. 2006b. *A centralized model for the regulation of anonymity online.* Working paper presented at European Computing and Philosophy conference 2006.

Wikipedia. 2007. *Blocking of Wikipedia in Mainland China*. http://en.wikipedia.org/w/index.php?title=Blocking_of_Wikipedia_in_mainland_China (accessed July 18, 2007).

Zittrain, Jonathan, and Edelman, Ben. 2003. Internet filtering in China. *IEEE Internet Computing* 7(2):70–77.