

Internet Censorship: The End of Digital Libertarianism?

OMER TARIQ

Candidate for MSc

Department of Information Systems

London School of Economics

Cyberspace regulation has recently emerged as a hot topic in media as well as the academic discourse in legal and socio-political study of Information Systems. Regulation of cyberspace is primarily defined by state-controlled Internet filtering, but there are other forms of control at various levels. This paper aims to investigate cyberspace control from the modalities of regulation perspective, looking at the various forms of control exercised by the state directly as well as indirectly through non-state actors. The control of governments over Internet has put to rest the views of Internet as libertarian architecture, out of jurisdiction of governments. No state allows its citizens completely unrestricted access to information. The reality on ground is that states shall try to vet what type of information on the Internet is allowed to its subjects. There is a need for understanding the methods by which state controls the Internet in order to make it more resilient against state regulation.

The justification and reasons for studying the Internet

“Is the coverage being given to Internet in media and academic discourse justified?” one may ask. There have been other media relaying information on large scales that were not covered in similar manner. Why then is the Internet deserving of so much attention? (Sommer, 2001) questions the sanity of considering the cyberspace as ‘legally central.’

There is, however, evidence to back the case for serious consideration of the Internet. Emphasis, in the new economy, is on exploring new methods of value creation. (Clippinger & Bollier, 2003) while discussing the need for new value creation methods, quote Internet law experts David Johnson and Susan Crawford pointing to the blindness of human being to the Internet as proof that value can be created by working together, uninitiated by government action or exploitation of private property, markets or firms.

Another reason for serious study of the Internet is the fact that governments around the world are making proactive efforts to control it. Embedded within the code of the Internet are features that make it a very fast and relatively intractable medium than traditional forms of media (Shapiro, 2000). These are:

- many-to-many forum: In contrast with traditional broadcast-based media (radio, television and the press), the Internet is a many-to-many medium. This is most evident in P2P and online communities.
- digital content: The digital nature of internet content makes it easier to replicate and mirror to new destinations thus making it hard for governments to control.
- distributed and packet-switched architecture: The fact that data is divided into packets that can each take any of various channels to reach the destination makes it easier for users to route around filtered gateways.
- interoperability: The compatibility of the underlying software and hardware with each other increases the reach of the Internet. It also becomes harder for the government to control the Internet by disallowing specific applications.

(Shapiro, 2000) also mentions broadband and universality as additional features. While broadband increases the size and

type of content that could be accessed from Internet, universality is more a ‘right’ that has yet to be achieved. Again the design of Internet and Web makes it open and accessible to anyone able to connect to it but ideas like the digital divide address the gap between the digitally privileged and the have-nots.

The above features of the Internet – any form of content can be uploaded anywhere in the world and accessible instantly to a large number of people and be easily mirrored - make governments feel more threatened and react to controlling it. Certainly the unrestricted flow of hundreds of gigabytes of data is much more worrisome than a hundred or so copies of a book, magazine or video. These features form what is known as the architecture of the Internet, which (Lessig, 1998a) mentions as one of the four modalities of regulating an entity. Before proceeding with further discussion of Internet control, we shall discuss the four modalities of regulation and the ecology of regulation based on the New Chicago School (Lessig, 1998a).

Four Modalities of Regulation

(Lessig, 1998a) mentions four modalities that can regulate an entity – law, market, norms and architecture. Law is a way to directly control an entity, by banning its very use or production. Markets help to increase prices or create or reduce demands. Norms may discourage people. The most interesting modality though, is architecture, also known as nature or code which regulates an entity by its design. In the “New Chicago School” however, law not only regulates directly but also indirectly by regulating the three other modalities.

The “New Chicago School” establishes regulatory links between law and the other modalities. It is a more realistic model as it sees government using law to control the other three modalities and using them together for better control and regulation.

This distinction of views in the old and new Chicago school was instrumental in defining two different perspectives of Internet and the State. The first view, of which Robert Perry Barlow (of the Declaration of Independence of Cyberspace fame) is the most well-known proponent, takes note of the

embedded features of the Internet discussed above, and sees them as opposing forces to governments trying to control Internet through law-enforcement (Barlow, 1996). It sees freedoms of Internet users – a digital- or cyber-libertarianism – guaranteed by its design. It encourages the designers of Internet-based applications to continue the service to the public by making its architecture more conducive to freedom.

The second view describes this libertarianism as a hype of cyberspace (Lessig, 1998b). Governments are regulating the Internet by using other modalities, of which architecture is the most significant. It suggests that in addition to increasing the integration of the three modalities (norms, markets and architecture) with the Internet for increasing its freedom-of-use, their susceptibility to state regulation should be noted and efforts should be made to make them resist it.

(Boyle, 1997) uses Foucauldian analysis to discredit digital libertarianism. Whereas digital libertarianism proposes cyberspace as an alternative sovereignty to that of the State, Boyle points to Foucault's challenge to the vision of power as sovereignty with a vision of surveillance and discipline. Control of architecture, especially by monitoring and filtering its usage, is the most common regulation in the case of the Internet. As shall be seen from cases discussed in the next section, the State is most interested in using law to regulate the architecture of Internet. This is also because Internet is a heavily architecture-based technology. And controlling its architecture is probably the most effective way for governments to control it while allowing to maintain (or trying to maintain) a good image. Quoting Mitchell Kapor of the Electronic Frontier Foundation from (Reagle, 1998), "Architecture is politics."

Internet Censorship

The architecture of the Internet is constantly evolving. One problem in law regulating the Internet directly is this very supposition that the architecture of cyberspace is static. This was most evident in the episode regarding the US Communications Decency Act (CDA), which was signed by Presidential decree in 1995 only to be made void by the Supreme Court 16 months later. The Act made the deliberate transmission of "indecent" messages to anyone under the age of 18 an offence punishable by law. One of the reasons cited by the US Supreme Court in dismissing the Act was that technology to screen kids did not yet exist (Shapiro, 2000).

In real world America, mentions (Lessig, 1998), pornography distribution in minors is regulated by norms, markets and architecture as kids do not venture near dodgy areas, cannot afford to pay the price to acquire such material and certainly cannot dress up as adults to hide their ages. The architecture of the Internet of 1995, however, could not screen kids from accessing indecent material. The Internet of 1995 was the Internet depicted by the New Yorker cartoon (Steiner, 1993) showing a dog using a computer with the caption "On the Internet no one knows you're a dog." A more recent cartoon on the Web shows a dog on a computer with the screen welcoming him with his personal data and personality traits (UNC, 1997) - a "reality check" into the architecturally changed Internet. Credit cards are now used to screen kids to adult-only services on the Internet.

The first generation of Internet control involved using the law. The CDA mentioned above was one such instance. In Ger-

many charges were brought up against Internet Service Providers (ISP's) and a student for disseminating offensive material (neo-Nazi propaganda and leftist literature, respectively) (Shapiro, 2000). In China, where government-opposed or banned movements like Falun Gong relied heavily on the Internet for mobilization of their members, government dissidents Lin Hai and Huang Qi were arrested and tried with wide coverage of their trials in media so that their fate was widely known.

States started moving towards indirect control via architecture soon after the first wave of Internet controls. Verdicts of legal cases often ordered measures to control access on parts of ISP's. The German ISP CompuServe whose head was fined \$60,000 USD and announced a 2-year suspended jail sentence required the ISP to monitor user activity online. In Iran a crude regulation of the Internet was carried out when, according to a report by Human Rights Watch, the government opened online chat-rooms where only two people could converse with each other. Other cases of (ethically questionable) interference in architecture were noted in China where, according to a study carried out in 2002 users requesting the URL www.google.com were redirected to other search engine pages. Later the government was found to be using a different strategy where search requests were passed through a proxy server and, if found to be searching for specific keywords, users would end up losing their Internet connection for a time period that ranged from a few minutes to hours (Zittrain, 2004). In other instances users requesting specific sites got "technical errors" (socket errors, and time-outs), making it hard to tell whether the site was actually blocked or undergoing down-time.

The Chinese government handling of Internet censorship is different from that of the Saudi government in two ways - transparency and formalization. In Saudi Arabia, where the government did not allow Internet access to citizens until it had installed filters (Shapiro, 2000) and where a large number of non-sexually explicit sites were blocked including proxy-circumventing websites, there is a clear definition of banned content and access to a blocked sites redirects the user to a webpage explaining the government's content filtering process. According to (Zittrain & Edelman, 2002), the user is allowed access to a feature where he can request unblocking or blocking of web content.

Transparency is in fact a salient feature of recent indirect Internet regulation methods. One form of refined indirect Internet regulation is by the recent mushrooming of Google's localized services. As an alternative to having its site blocked or its queries interfered by local service providers, as in China, Google has now opened localized services in various countries where search results are altered as per government recommendations. In an interview given to *Playboy* in September 2004, while Google co-founders had expressed knowledge of their site being blocked in China and later allowed due to huge public demand, they had stated they were not happy with policies of other search engines that had established local presence in the country and were offering restricted information to users. Google now offers a similar "restricted service" in China since January 2006 with sensitive information removed while stating, on the official Google blog, that it was "not an easy choice" and that they "aren't happy".

However one difference between Google's current services at

www.google.cn is transparency. A result on searches with black-listed keywords returns the following text in Chinese at the bottom of the page:

据当地法律法规和政策，部分搜索结果未予显示。

“According to the local legislations and policies, some of your search results are not available.” (text searched: “Tiananmen square”)

This type of transparency is also found on other Google sites. A search for “The American Nazi Party” in www.google.fr results in:

En réponse à une demande légale adressée à Google, nous avons retiré 5 résultat(s) de cette page.

“A legal claim required removal of 5 search results.”

The US government in the past has, in a reaction to the availability of strong encryption technologies, tried to promote and force weaker encryption standards by persuading standard-setting bodies to promote them as well as giving incentives to manufacturers. Manufacturers of the “Key Escrow” encryption standard were provided with incentives such as relaxed export controls for software using the standard. This was a case of using the market indirectly for regulation.

The way ahead

The acceptance of indirect regulation of the Internet points to a number of propositions for making progress in cyberspace freedom. (Samuelson, 2000) mentions five challenges for regulating the Global Information Society – the need for new laws and policies, proportionality, flexibility, preserving values and trans-national co-operation. The need for new policies is easier to decide once we accept the state’s desire to control Internet directly via laws and indirectly via norms, markets and architecture.

Proportionality and flexibility point to the need for new policies to not be over-protective and be designed with a simple and minimalist character. In a recent talk at the Oxford Internet Institute’s Research and Policy Workshop Professor Jonathan Zittrain mentioned four “Principles of Censorship” that would promote acceptable Internet controls. These are transparency, formalization (both of which are exemplified in the discussion on the Saudi filtering regime above), limitation of scope and reduction of collateral censorship.

Preserving values and transnational cooperation are more political in nature. When emphasizing on preserving values, it is important to not stay put on values of a certain culture and export those values abroad. Values held by certain states based on ethnic, social or religious reasons demand as much respect as those upheld by others, based on freedom and individualism. The Internet can be a source of learning of new cultures which can bring about a slow change, but it should not be used as a tool to thrust institutionalized values and beliefs, no matter how progressive or modern, to foreign lands. Transnational cooperation requires countries to concentrate on policy goals rather than the means to achieve them. An example is transparency where individual countries may restrict content as per state policies, but ensure the policies are well-known to the general public. Once policies are out in the open, it would be easier for them to be discussed and ultimately be aligned with the values of the local population.

(Shapiro, 2000) mentions that indirect control of Internet allows governments to easily get away with what they want to do without problems like constitutional limits or public outcry. He blames “obscure committees” behind communication protocols and standards, comprising of technical professionals, mainly engineers and computer programmers, as the reason for government’s hijacking of these committees for their own motives. The New Chicago School points to the need for making the architecture and other modalities resistant to law. This would require adequate thinking on the social and political implications of technology while drafting standards and designing new technologies.

Conclusion

The article looked at the New Chicago School model as a better way of understanding the realities of Internet regulation by the State than digital libertarianism. It looked at the types of Internet Regulation in various locations for evidence of applying the New Chicago School model to it. As a result, most current Internet Censorship can be attributed to the state’s indirect regulation by regulating the architecture of the Net. Various measures and guidelines are mentioned as the way forward towards a more info-democratic model of the Internet. The New Chicago School allows us to appreciate the link between architecture, norms and markets with law. A more globally accessible Internet would require more resistance to be built into the Internet from the point of view of these methodologies to make them more defiant from being regulated by law.

References

- Barlow, J. P. (1996); A Declaration of the Independence of Cyberspace. <http://homes.eff.org/~barlow/Declaration-Final.html>
- Boyle, J. (1997); Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-wired Censors. *Univ. Cin. Law Review* 66: 177. <http://www.law.duke.edu/boylesite/foucault.htm>
- Clippinger J, & Bollier, D(2003); A renaissance of the commons: How the new sciences and Internet are Framing a new global identity and order <http://cyber.law.harvard.edu/people/RenaissCommon12.07.03.pdf>
- Lessig, L. (1998a); “The New Chicago School.” *Journal of Legal Studies*. 27 (June): 661-691.
- Lessig, L. (1998b); The Laws of Cyberspace. Proceedings of the Taiwan Net ‘98 Conference, Taipei, March 1998. http://cyber.law.harvard.edu/works/lessig/laws_cyberspace.pdf
- Mclaughlin, A (2006) Google in China, Official Google Blog – 1/27/2006. <http://googleblog.blogspot.com/2006/01/google-in-china.html>
- Reagle J (1998); Why the Internet is Good? Berkman Center Working Draft. <http://cyber.law.harvard.edu/people/reagle/regulation-19990326.html>
- Samuelson P (2000); Five challenges for regulating the

- Global Information Society in Regulating the Global Information Society. Routledge, London.
- Shapiro, A. L.(2000); The control revolution : how the Internet is putting individuals in charge and changing the world we know. New York: Public Affairs, NY.
- Sheff, D (2004); Google Guys: A candid conversation with America's newest billionaires about their oddball company, how they tamed the web and why their motto is "Don't be evil," Playboy Magazine (September 2004).
<http://www.secinfo.com/d14D5a.148c8.htm#1ovvc>
- Sommer, J. S.(2001); Against Cyberlaw, Berkeley Technology Law Journal Vol 15 No. 3, (pg 1145-1232).
- Steiner P (1995) "On the Internet, nobody knows you're a dog" New Yorker.
<http://cyber.law.harvard.edu/people/reagle/dog.jpg>
- UNC (1997) "A Reality Check"
<http://www.unc.edu/depts/jomc/academics/dri/sum97/dog2.gif>

- Zittrain J (2004) China and Internet Filters: When the reporting of major news organizations is blocked, why not do something about it? Nieman Reports, Summer 2004. (pg. 105-107).
- Zittrain J and Edelman B (2002) Documentation of Internet Filtering in Saudi Arabia, Berkman Center for Internet and Society, Harvard Law School.
<http://cyber.law.harvard.edu/filtering/saudi Arabia/>

ABOUT THE AUTHOR

A graduate of the GIK Institute of Engineering, Pakistan, Omer Tariq worked as a Network Engineer with an IT reseller in Abu Dhabi, UAE which is also where he was born. His interests are the role of ICT in developing countries and the control and monitoring of the Internet. His dissertation is on the role of IT Higher Education in bringing about socio-economic progress in developing countries.