Virtual Censorship: Controlling the Public Sphere

Mathias Klang
Informatics, IT-University, University of Goteborg, Sweden
klang@ituniv.se,
http://www.ituniv.se/~klang

Abstract: This article deals with online censorship and its relation to user autonomy. By presenting censorship practices and activities of groups helping to circumvent censorship this article shows that the regulation of online material is an ongoing process between the regulator and the regulated. The result of this process is the way in which a society defines itself in terms of a free and vibrant democratic public space.

Keywords: censorship, regulation, public sphere, user autonomy

1 Regulating Disruptive Technology

While the discourse on the regulation and control of technology has an older pedigree [1, 2] much of the discussion in relation to the Internet developed in polemic to Lessig's [3] concept of four modalities of regulation. Murray and Scott [4] further developed Lessig's concepts by in an attempt to create a theory that will encompass the largest range of regulatory strategies and instruments [5].

The incentive to regulate Internet technology has received strong support after the terrorist acts of 9/11, which had a direct affect upon the limitation of online civil liberties. Since then, several governments have moved to implement and extend anti-terror regulation. Hamilton [6] defines three main areas were these activities are taking place (1) the creation of a data retention structure, both at national levels and through international co-operation. This entails the mandatory requirement that Internet Service Providers (ISP) store all user data for specific periods. (2) Online surveillance – regulation in this area is making surveillance technically possible and formally easier. (3) Direct censorship – because "terrorists should not be able freely access sensitive information…" [6].

The desire to control online information stems from the understanding that ICT is a disruptive technology [7]. As such, it is fundamentally altering the way in which

we organize ourselves socially; not all welcome this disruption. This article presents the examples of attempts to regulate online information and reactions to these attempts.

This article begins with an explanation of socio-technical censorship practices, followed by a description of the actions of groups attempting to provide anti-censorship techniques and technology. The discussion shows how the actions of the regulators and regulated form part of a technology negotiation where social groups are attempting to come to terms with the disruptive effects of Internet technology in relation to the democratic ideals of freedom of information and autonomy.

2 Censorship Practice

Internet content filtering is the process of preventing user access to information on the Internet most filtering systems focus on the world wide web by software placed between the user and her Internet connection [8]. For the most part filtering is dependent upon one of three techniques. The different techniques can be used in combination to achieve the desired effect. The processes are known as *blacklisting*, *whitelisting* and *content analysis*. Blacklisting refers to the process whereby lists of unacceptable websites are collected. Once the filtering software is installed, the software will first check to make sure any website requested does not occur on the list of websites collected on the blacklist.

The use of blacklists entails handing over power and decision-making capacity to another agent. Commercial blacklisting products have received a fair amount of criticism for their tendencies to overblock (i.e. to block more access to more information than necessary). A recent study found that in school blocking software "for every web page correctly blocked as advertised, one or more was blocked incorrectly" [9].

Whitelisting is also a process of allowing access to material that has been checked in advance. Under this system, users are permitted access to material that has been approved in advance. This method is more cost efficient in terms of limiting user access to unwanted information. It also is prone to overblocking, i.e. it blocks more information than intended and thus mitigating the potential of the communications technology.

The third form of filtering is content analysis. The concept behind this system is to avoid predefined lists (irrespective of whether they are black or white) and to focus on the actual content of what is viewed. Content analysis works by setting predefined characteristics of the material, which is to be avoided, and allowing software to scan the information for this content prior to delivering it to the user.

If the software is programmed to recognise sexually explicit language and the user attempts to view a page which such content, access to the page will be denied. This system has obvious appeal since it avoids the pitfalls of white & blacklisting. The system brings with it problems of its own. Content analysis is not a substitute for understanding information in context. If keywords are used then sites may be unintentionally blocked. For example, the city of Scunthorpe has been blocked since the word contains within it a four-letter word. Other content analysis systems

intended to prevent access to sexually explicit material have blocked sites containing images with large amounts of skin-coloured pixels. These systems have been known to block close up pictures of a non-sexual nature (such as headshots) since the bulk of the image consists of skin-coloured pixels.

State of the art filtering software usually attempts to use a mixture of these three systems and include a level of human activity to 'teach' the filters the items to block and to accept. As these examples have shown, there is no such thing as a system that will not over- or underblock. Therefore, systems will always be either tools of conscious and inadvertent censorship or less than 100% efficient.

In a study conducted by Deibert and Villeneuve [10], they show online censorship activities carried out by 22 states. They divide these censorship activities into three categories (1) comprehensive censorship, (2) distributed censorship, and (3) limited censorship. Comprehensive entails a large-scale censorship activity, distributed censorship refers to a significant amount of censorship performed, and usually the actual act of censorship is delegated to the ISP. Limited censorship refers to, as the name implies, small amounts of censorship.

While there is a great deal of concern about the states who traditionally censor the Internet such as China, Cuba, Myanmar and Turkey etc there are other states which appear on the list which are traditionally not understood to be censorship states. Such states include the USA, France, and Germany. These states rarely receive the same amount of bad publicity for their censorship since it is commonly understood that these states are for freedom of information. It is easy to see how this stance becomes problematic since even these states censor access to information online.

There seems to be two main approaches among States implementing comprehensive censorship practices. Myanmar and Cuba limit access to the Internet by ensuring that only limited numbers of individuals can go online and even those who can may only see approved material – the rest is filtered [10]. China, Saudi Arabia, and Turkey are more permissive when it comes to allowing individual's access to the Internet but the content they are allowed to view is heavily filtered [10]. Additionally these countries attempt to register those who access the Internet through Internet cafés.

Among those who are less ambitious in their filtering activities, we find that ISP's, or in the case of the USA libraries, are required to filter different types of content in an effort to protect certain cultural values. Often the filtering is heavily focused on, but not limited to, preventing pornography. The filtering of dissident and human rights sites follows this in a close second place [10]. Those who filter least, according to Deibert and Villeneuve (2005) are countries like France where courts have ordered Yahoo! to block access to Nazi auction sites, Germany in which certain states require ISPs to block Nazi sites, and Jordan, which blocks the site of arabtimes.com at a national level [10].

What Deibert and Villeneuve's [10] study clearly shows is that it has become increasingly difficult to speak of censorship in terms of them and us. Many states, traditionally accepted as pro-free-speech, censor to a lesser or greater degree. That the more censorship-friendly states such as: Turkey, Cuba and China filter information is not a great surprise. It is important in all these cases to remember that

no matter how well planned and organised the system of censorship is – there is no such thing as a perfect system.

Privatized Censorship

While we can understand relatively easily much of the censorship carried out in terms of central powers controlling the flow of information in the attempt to achieve certain political goals, not all Internet censorship follows this pattern. Two main areas of concern, which fall into the category of private censorship, are the role of the Internet Service Provider (ISP) and legislation with a chilling effect [11].

Censorship by ISP can take many forms, but most generally fall into one of two categories. Either the censorship occurs as part of a governmental recommendation or requirement or the censorship is a part of corporate policy – which may in turn be a part of industry self-regulation or simply an individual corporation policy. One example of such as policy is the Public Pledge of Self-Regulation & Professional Ethics for China Internet Industry, which states that the principles of self-regulation and the Internet industry's professional ethics include "…patriotic observance of law, equitableness, trustworthiness and honesty" (Article 3). The duties created by the pledge involve refraining from, and actively monitoring that customers do not, produce, post, or disseminate material that may jeopardize state security and disrupt social stability, contravene laws and regulations and spread superstition and obscenity. One must promptly remove any such material.

The public pledge is written as a one-sided declaration from the corporate actor. This creates the image that the corporate actor has the choice to refrain from signing the document, declaring support for it or implementing it in any manner. The non-implementation of the document is understood to bring with it additional difficulties for companies intending to enter the Chinese Internet market. Therefore, companies follow the Public Pledge, which results in the inspecting and monitoring of national and international sites and blocking access to harmful content as stated by Article 10 of the Public Pledge.

In January 2006, Google launched a local version of its online search engine for China (Google.cn). This version will block 'subversive' content from the Chinese users and therefore help Chinese officials to filter Internet content. Especially since to large degree today any website not listed by search-engines has little chance of users finding it. This addition to the Chinese censorship technology has the effect that even sites which are not caught by the Chinese firewalls [8] can now be excluded since they are not part of the material that can be found when using the search engine. Google made several statements in response to the protests over their actions.

> …we have agreed to remove certain sensitive information from our search results...This wasn't an easy choice, but in the end, we believe the course of action we've chosen will prove to be the right one…We ultimately reached our decision by asking ourselves…how can we provide the greatest access to information to the greatest number of people? [12]

The threat presented by the privatized censorship of service providers should not be underestimated. Today the online search engines have become the de facto standard for finding online information and online navigation. These search engines are not a form of public good. Many consider the search-engine as a technology and as such neutral. This view omits the fact that the technology exists in a corporate context with a duty to create profit [13]. Despite the search engines role as fundamental infrastructure they are driven by profit motives and therefore no obligation to ensure equal access to information. The effects of privatized censorship are that a greater amount of information becomes unavailable. Once the opposing views are made unavailable, what remains online is a form of consensus. This makes it even more difficult for anyone harboring an opposing view to speak out. In addition to this the harm of privatized censorship is made more grave by the fact that there is little or no information about the censorship rules, therefore the ordinary user cannot be aware of what is censored and therefore cannot realize when she should attempt to circumvent the censorship.

The second category of private censorship is the case of regulation with so called chilling effects, in other words the stated purpose of the regulation is not to limit a certain action (such as free speech) but has that as a negative side effect. This may sometimes fall outside the strict definition of censorship, the effect of legislation, which prevents the ability of communication; it results in the lessened flows of free information. While it is important to mention this topic here, due to space constraints it is not possible to give the topic the attention it truly deserves. Many different bodies of legislative rules may affect the way in which communication occurs. Those that are most common are privacy [14], defamation [15], copyrights [16] and trademarks [17]. The importance of bringing up the topic of the chilling effects of legislation is to underline the difficulties that the communicator faces. The problem is not in the rules but in their interpretation and implementation. When taken at face value the regulations do not vary greatly. One can easily implement their achievements in such a manner as to entirely prevent or cause a chilling effect on the actors.

3 Circumventing Censorship

In an early work on Internet censorship Varlejs [18] discussed which actors were carrying out Internet censorship and for which purposes. Listing actors involved in censorship as governments, academic institutions, religious groups, corporations, media and libraries, Varlejs [18] notes that these actors censor different types of information, for different methods and motivate it through different rationales.

The focus of this work is on Internet content and the limitation or control of the free flow of information it is important to be aware of the technologies of information control available to the controller. The first important difference between the traditional censor and Internet-based censorship is that the information in question has usually already been disseminated. Therefore, the focus is not what we may disseminate but rather how to prevent groups from accessing this information. The main process involved in this activity is one of filtering. The term

is aptly chosen since the activity involves allowing the free flow of acceptable material while preventing the harmful content from being accessed.

The evasion of censorship has always been a popular topic [19]. One can almost see this as an escalating race of technology. For every move, the censor carries out to implement new forms of censorship technologies and techniques there is a rapid move towards new and better forms of hidden communication. The advent of the Internet has increased the amount of cheap international communications distributed. The race to censor and to beat the censor has been going on for some time but it is still in its infancy.

Information on censorship evasion also tends to focus on the use of pseudonyms and maintaining a level of secrecy to ensure that if communications are intercepted the communicants will not be able to be identified and punished. There are, naturally, two sides to these arguments. The use of such techniques by those who cause harm is abhorrent while the use of these techniques by those who bravely fight for freedom is praiseworthy. The question then becomes one of degree and definition. Which user causes harm and which users are actually praiseworthy? Much of the activities we deplore today were historically acceptable and there is no reason to think that these decisions have been, or will ever be fixed.

Therefore, censorship becomes a point of view. Those who are against and those who are for are solely demonstrating differences of opinion and serendipity is the only thing that places us on one side of the barrier or the other. This argument from cultural relativism is not an adequate argument to prevent activity on both sides of the fence. Since we may interpret the concept of censorship as a point of view, several actors have been moving towards creating technical anti-censorship devices. The object of these is to help avoid state censorship without detection. One example of such a system is Freenet.

Freenet [20] is software designed to enable the publication and retrieval of Internet based information without fear of censorship and distributed at no cost. This is done by creating a completely decentralised network where information about publishers and consumers of information is anonymous and not stored. The advantages of decentralisation is that no single point controls the network and the advantage of anonymity is that users can depend on the network for communications without fear of advance censorship or post-publishing reprisals. In addition to encryption, communications travel through several nodes to make tracking the information requester more complex. According to the project site, people have downloaded the software several million times and have used it in countries with comprehensive censorship systems.

In addition to the development of technical anti-censorship technologies there have been social actions developed to help with censorship evasion. These have taken the form of publications with the activist as a target audience. The goal is to provide readily available information about censorship and to avoid or mitigate its effects.

The online civil rights organisation Electronic Freedom Frontier (EFF) has produced a guide to ensuring blogging safety that is aimed at ensuring that those who create online information do not meet with negative consequences from employers or state censors. Their advice includes [21] using pseudonyms and limiting the use of identifiable information, promoting the use of ‘anonymizing’ technologies, and using

ping servers to publish information then quickly removing it (the effect is that the information remains on other servers but not on the publishers site). In addition, the advice includes limiting audiences through password-protected sites, avoiding being included in search engines, and registering domain names anonymously.

The EFF has a high reputation for civil liberties work and it has been active online since 1990. The organization has a large audience and deals with a wide range of issues pertaining to online civil liberties. The motivations for producing such documents are to ensure that the individual can act autonomously in providing and receiving information without fear of outside coercion. They write:

> …we offer a few simple precautions to help you maintain control of your personal privacy so that you can express yourself without facing unjust retaliation. If followed correctly, these protections can save you from embarrassment or just plain weirdness in from of your friends and co-workers. [21]

Hence, the underlying belief is that the individual should have the choice to publish information but this choice or desire is limited by the potential threats the individual faces if such activities are carried out. The EFF publishes several documents of this nature on their website ranging from legal to technical advice intended to empower the individual and provide tools to ensure individual informed choice. In addition, documents such as this also fulfil a political purpose by sustaining and contributing to a larger debate on online freedom.

The EFF takes the civil liberties stance and individual actors provide information without attempting to place their work in a larger ideological context there have also been moves from non-Internet organisations to help circumvent online censorship. One such organisation is Reporters Sans Frontiers (RSF). This organisation focuses on freedom of the press. However, it also has developed an interest in protecting a larger group, namely the non-professional reporter using the Internet to publish and disseminate information online. To this end, RSF has created an anthology [22] that includes introductory texts on information activism with information on topics such as how to get started, which are the best tools and what ethics bloggers should have. In addition to this the handbook gives example cases of what bloggers have been able to achieve before offering concrete advice on anonymous blogging [23] and censorship circumvention [24].

Zuckerman [23] discusses social safety precautions similar to those seen above [21] i.e. using pseudonyms, public computers and anonymous proxies before moving on to the more advanced precautions such as union-routing and using anonymous blog services involving encryption, re-routing and anonymous re-mailers. The main point Zuckerman [23] is attempting to make is that anonymity is possible; however, for each step there is a cost in time or learning required to be able to use the tools. Hence, the trade-off becomes a factor of risk evaluation, knowledge, and time. Depending upon the underlying risk, it may become worthwhile to invest time and energy in learning to use the available tools. Villeneuve's [24] focus is on circumventing online filters, therefore after a brief introduction to filtering he presents a spectrum of circumventing technologies and a methodology for the user in determining the right balance between the users needs and capacities. The results of such an evaluation determine the course of action and the focus needed for

developing circumvention methods and avoiding detection. The choice of circumvention method will be based upon factors, such as, number of users, bandwidth availability, point of access, levels of expertise, and the risks being undertaken. Once determined Villenueve [24] presents an array of web-based circumventors, circumvention through proxy servers, tunnelling and the wide-scale anonymous communications systems.

4 Discussion

Autonomy is accepted as a core democratic value and it is often argued that in the absence of compelling evidence to the contrary, everyone should be treated as the best judge of his or her own good or interests [25, 26]. Freedom of information is a fundamental building block in supporting the autonomous actor [27]; therefore the ability to find and communicate information is the basis upon which the democracy is built. This position has been uncontested by most nations for a long time. One may argue that the change is not in the concept but rather in its practice. Prior to the advent of the Internet the ability of the individual to communicate with large groups was not great.

The components defining access to public sphere [28] include (i) physical access, (ii) social access, (iii) access to discussions, and (iv) access to information [29]. Castells [30] presents the idea that the public sphere has, to all intentions and purposes, moved from the physical world to the network. Therefore, it is important to look to those writers who claim that the Internet is the public sphere and then to attempt to understand whether or not the same rules apply to the autonomous participant.

This is the continued negotiation between regulation and technology. This may deal with the adaptation of social behavior (or implementation of technologies) to coincide with regulation or attempts to evade the effects/sanctions prescribed by regulation or the behavior of following the wording of the legislation while ignoring its substance. These negotiated socio-technical solutions attempt to either circumvent regulation completely or at least to cushion its effects.

The issue is one of user autonomy in online environments. The ability to act without coercion or manipulation is vital to democratic participation. This is true even in the online environment. By implementing direct control over Internet content through online content filtering or implementing regulations through industry codes of conducts which require such filtering to be carried out by private actors directly impacts online autonomy. The same can be said of the actions of search engines such as the case of Google.cn, mentioned above, since removing information from the search engines effectively makes the information invisible to the larger public. If the information is not available through search engines it is, for all intents and purposes, not there at all. Without the ability to locate and gather information the individual cannot acquire the adequate information necessary to make autonomous decisions based upon the facts. Therefore through manipulation the public information sphere cannot function.

The promise of efficient communications and the development of the Internet into a public sphere without the limitations inherent in Habermas' [28] model have quickly been proven to be false hopes. Reactions to censorship have caused many to both protest and react towards the threats against online autonomy. These reactions come both in technical solutions and in attempts to educate users on the importance of security and risk awareness to prevent autonomy loss.

5 Conclusion

ICT carries with it many promises for democracy. Despite this, technology is also being implemented to limit the scope of autonomy among ICT users. The present situation is one where many parties are conducting the regulation of online communications and Internet user groups are helping each other communicate and circumvent controls that prevent communication. The result of this negotiation between the regulator and regulated is the development of understanding of information in the digital age.

By understanding online information flows as a disruptive technology it is possible to arrive at a more nuanced understanding of that which is regulated. By recognizing that disruptive technology is as uncontrollable as an 'earthquake' [7] the regulator must understand that suppression is not an adequate solution to the problem.

As this work has shown, the negotiation is an ongoing process without end. Once techniques are developed to block information countermeasures will be devised and implemented. This result of this process is fundamental to the way in which we define the modern democracy.

Bibliography

1. J. Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society*, Harvard University Press, Cambridge, Mass., 1986.
2. J. Yates, *Control Through Communication: The Rise of System in American Management*, Johns Hopkins University Press, Baltimore, 1989.
3. L. Lessig, *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999.
4. A. Murray, and C. Scott, The Partial Role of Competition in Controlling the New Media, *Proceedings of Competition Law and the New Economy*, University of Leicester, 2001.
5. R. Brownsword, Code, Control and Choice: Why East is East and West is West, *Legal Studies*, **25 (**1), 2005.
6. S. Hamilton, The War on Terrorism – Towards a 'less free, less choice' Internet for Library Users? *World Library and Information Congress: 69th IFLA General Conference and Council*, 2003.
7. K. Lyytinen and G. Rose, The Disruptive Nature of IT Innovations: The Case of Internet Computing in Systems Development Organizations, *MIS Quarterly*, **27** (4), 2003.
8. J. Zittrain, and B. Edelman, Internet Filtering in China, *IEEE Internet Computing*, **7(**2), 2003.

9. EFF & OPG, Internet Blocking in Public Schools: A Study on Internet Access in Educational Institutions, Report from the Electronic Frontier Foundation (EFF) and the Online Policy Group (OPG), Version 1.1 of 26 June 2003.
10. R. Deibert and N. Villeneuve, Firewalls and Power: An Overview of Global State Censorship of the Internet, in *Human Rights in the Digital Age* edited by M. Klang and A. Murray, Glasshouse Press, London, 2005.
11. J. Boyle, *Shamans, Software & Spleen: Law and the Construction of the Information Society*, Harvard University Press, Cambridge, Mass. 1996.
12. A. McLaughlin, Google in China, in *Google Corporate Blog - Googler insights into product and technology news and our culture*, 27 January. 2006, http://googleblog.blogspot.com/2006/01/google-in-china.html – consulted 1 April 2006.
13. M. Friedman, The Social Responsibility of Business is to Increase Its Profits, *New York Times Magazine*, 1 September 1970.
14. N. Taylor, State Surveillance and the Right to Privacy, *Surveillance & Society* **1**(1): 66-85, 2002.
15. C. Dent and A. Kenyon, Defamation Law's Chilling Effect: A Comparative Content Analysis of Australian and US Newspapers, *Media & Arts Law Review*, **9(**2): 89-112, 2004.
16. M. Heins, The Progress of Science and Useful Arts: Why copyright today threatens intellectual freedom, Free Expression Policy Project (policy paper), 2003.
17. S. Dogan, and M. Lemley, Trademarks and Consumer Search Costs on the Internet, 41 *Houston Law Review:* 777-838, 2004.
18. J. Varlejs, Who Censors the Internet and Why? *Proceedings of Freedom of Expression, Censorship and Libraries*, Riga, Latvia, October 14-17, 1998.
19. S. Curry Jansen, *Censorship: The Knot that Binds Power and Knowledge*, Oxford University Press, Oxford, 1991.
20. I. Clarke, and O. Sandberg, Routing in the Dark – Scalable Searches in Dark Peer to Peer Networks *Defcon 13*, Las Vegas, July 2005.
21. EFF, How to Blog Safely (About Work or Anything Else), Electronic Frontier Foundation Report, 2005.
22. J. Pain, *Handbook for Bloggers and Cyber-Dissidents*, Reporters Without Borders, 2005.
23. E. Zuckerman, How to Blog Anonymously, in *Handbook for Bloggers and Cyber-Dissidents*, Reporters Without Borders 2005.
24. Villeneuve, N. (2005) Technical Ways to Get Around Censorship, in *Handbook for Bloggers and Cyber-Dissidents*, edited by J. Pain Reporters Without Borders, 2005.
25. R. A. Dahl, *On Democracy*, Yale University Press, New Haven, 1998.
26. T. Scanlon, A Theory of Freedom of Expression in *The Philosophy of Law*, edited by R. Dworkin, Oxford University Press, Oxford, 1977.
27. G. Dworkin, *The Theory and Practice of Autonomy*, Cambridge University Press, Cambridge, 1988.
28. J. Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*, translated by B. Thomas, MIT Press, Cambridge, Mass., 1989.
29. S. Carr, M. Francis, L. G. Rivlin, and A. M. Stone, *Public Space*, Cambridge University Press, Cambridge, 1992.
30. M. Castells, *The information Age: Economy, Society, and Culture*, Volume 1: *The Rise of the Network Society*, Blackwell, Oxford, 1996.