Can governments ever censor the web? A Literature Survey.

Reuben Binns

The web creates creates unique challenges and opportunities for governments wishing to censor content. The following annotated bibliography will present a range of disciplinary approaches to aspects of this phenomenon. As the papers collected here indicate, government censorship of the web already exists to a high degree in many countries. Therefore the question is not so much whether governments *can* ever censor the web, but rather how *effectively* can they do it.

Web censorship is here defined as the active prevention of citizens from accessing a given piece or type of web content. The question suggests an empirical rather than normative standpoint, and therefore in what follows I intentionally neglect a great deal of literature on the case for and against web censorship. Instead I focus on the *effectiveness* of government attempts at censorship. This could be taken as a purely technical question about what web censorship methods and tools exist, but the literature surveyed here suggests a broader approach looking at technical, legal and social factors. It therefore also involves a mixture of methodologies and disciplines. While drawing heavily from two disciplines (Computer Science and Law) it also includes perspectives from Economics, Socio-Legal and Political Science.

I categorise the research according to three main factors in a governments' ability to effectively censor web content.

1. The technical tools at its disposal and the nature of its communications infrastructure. Many of the papers which follow outline these tools, and some of the ways in which different infrastructures allow or inhibit censorship techniques.
2. The degree of success of citizens' attempts to circumvent government censorship, and how widely such circumvention is practised within the population.
3. Limitations of government power. These could be legal constraints limiting a governments ability to censor the web. They may be constrained by their constitutions, or membership in international federations such as the EU. There may also be limits to the level of government influence over key players in the private IT industry. Governments usually do not carry out all of the activities necessary to censor the web themselves, but rather rely on private entities to carry out censorship activities.

It is worth noting that there is often an ambiguity between the terms 'internet' and 'web', with some of the authors explored here using them interchangeably. Some of the techniques governments use to deny access to content involve interference at the level of the network, while others involve interference at the web level – for example in the domain name system. But the effect of both types of technique is the same – they deny access to content which would otherwise be accessible on the web, and therefore will be treated here as instances of web censorship. One reason the distinction is important, however, is that certain methods for the circumvention of web censorship (such as p2p filesharing of censored content) are not be web-based. In which case it could be argued that web censorship and internet censorship are distinct phenomena.

A note on the Web Science Subject Classification: I propose here to include the following additional category:

webscience.org/2010/E.6.2.7 Web Censorship

(Which would be a subcategory of: webscience.org/2010/E.6.2 Policy and Regulation)

Literature Search Methodology and Strategy

The literature search was carried out using the University of Southampton's research portal. Three key words from the question were identified – namely 'Government', 'Censor' and 'Web'. A preliminary search of the literature revealed that much of the relevant content employed related terms, namely “State”; “Block” and “Filter” (referring to types of censorship methods); and “Internet” (as stated above, “Web” and “Internet” are used interchangeably in some of the research papers). These terms were then dis-joined to the original search terms to increase the number of relevant results.

“Government OR State”
“Censor OR block OR filter”
“Web OR Internet”

These disjunctions were then conjoined into the following Boolean search sequences:

“Government OR State” + “Censor OR Block OR Filter” + “Web OR Internet”
“Government OR State” + “Web OR Internet” + “Censor OR Block OR Filter”
“Censor OR Block OR Filter” + “Government OR State” + “Web OR Internet”
“Censor OR Block OR Filter” + “Web OR Internet” + “Government OR State”
“Web OR Internet” + “Government OR State” + “Censor OR Block OR Filter”
“Web OR Internet” + “Censor OR Block OR Filter” + “Government OR State”

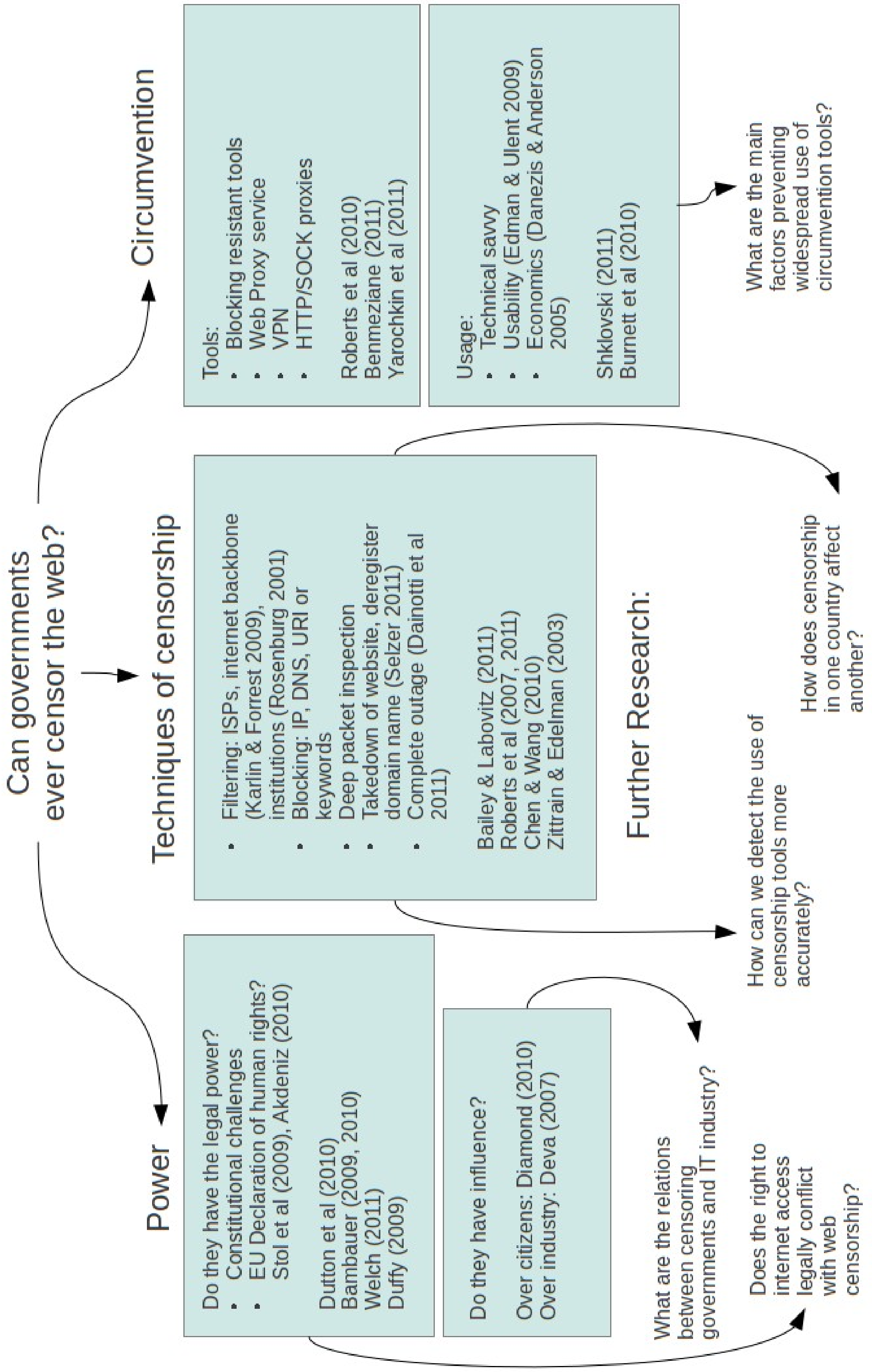
The point of exhausting the different search sequence orders was that certain database search algorithms use word order to determine the relevance of a given paper. Given that no set of keywords is more relevant to this question than another, each combination was used to ensure as many potentially related papers appeared in the search results as possible. In each database, the search was limited to journal articles, because these are more likely to represent in depth and cutting edge research, than books or other types of resource.

The following search databases were used:

TDNet
ACM Digital Library
IEEE Explore
Web Of Knowledge
Springer
Wiley
SSRN

A long-list of around 100 papers was selected from across the databases, further narrowed to 30 papers by scanning abstracts for relevance. Ten core references have been selected for further critical review.

<u>Literature Map</u>



Can governments ever censor the web?

Power

Do they have the legal power?
- Constitutional challenges
- EU Declaration of human rights?

Stol et al (2009), Akdeniz (2010)

Dutton et al (2010)
Bambauer (2009, 2010)
Welch (2011)
Duffy (2009)

Do they have influence?

Over citizens: Diamond (2010)
Over industry: Deva (2007)

Techniques of censorship

- Filtering: ISPs, internet backbone (Karlin & Forrest 2009), institutions (Rosenburg 2001)
- Blocking: IP, DNS, URI or keywords
- Deep packet inspection
- Takedown of website, deregister domain name (Selzer 2011)
- Complete outage (Dainotti et al 2011)

Bailey & Labovitz (2011)
Roberts et al (2007, 2011)
Chen & Wang (2010)
Zittrain & Edelman (2003)

Circumvention

Tools:
- Blocking resistant tools
- Web Proxy service
- VPN
- HTTP/SOCK proxies

Roberts et al (2010)
Benmeziane (2011)
Yarochkin et al (2011)

Usage:
- Technical savvy
- Usability (Edman & Ulent 2009)
- Economics (Danezis & Anderson 2005)

Shklovski (2011)
Burnett et al (2010)

Further Research:

What are the relations between censoring governments and IT industry?

Does the right to internet access legally conflict with web censorship?

How can we detect the use of censorship tools more accurately?

How does censorship in one country affect another?

What are the main factors preventing widespread use of circumvention tools?

Core References:

Dutton, W. H., Dopatka, A., Hills, M., Law, G. & Nash, V. (2010). ***Freedom of Connection - Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet*****. Paris: UNESCO, 2011**

This is an overview of the impact of government regulation on freedom of expression in 2010. The authors, who range from Computer Science to Socio-legal studies, draw together recent empirical research and case studies to provide 'a new perspective on the social and political dynamics behind threats to expression'. This report puts web censorship into the wider context of freedom of expression and access to information online. The authors propose an 'Ecology of Freedom of Expression on the Internet', which requires recognising that activities such as censorship necessarily involve the combined actions of multiple actors with a variety of goals. It also outlines recent trends around the idea and adoption of 'internet access as a human right', which represents a countervailing trend against censorship.

While the paper does not itself bring any new evidence to bear on the subject of web censorship, it makes an admirable attempt to bring all the existing evidence together. Chapter 5 takes data from two of the biggest surveys of web censorship around the world (from the OpenNet Initiative and Freedom House (2009)) to create a meta-study which provides an overall ranking of over 40 countries according to extent of filtering. However, as the authors rightly note, measuring level of filtering alone does not take into account what *kind* of material is filtered, which may be necessary to get a true picture of the effectiveness of web censorship efforts.

WSSC:
webscience.org/2010/E.5.3 Digital crime
webscience.org/2010/E.5.4 Laws for Web access
webscience.org/2010/E.6.2.7 Web Censorship

Stol, W.P. et al., (2009) Governmental filtering of websites: The Dutch case. ***Computer Law & Security Review*****, 25(3), pp.251-262.**

The authors assesses the technological, legal, and practical possibilities of blocking and filtering child pornography on the web, focusing on the Dutch government's attempts. It uses a combination of desk research, interviews with those responsible for filtering, and an on-site review of the filtering practice.

This paper is important because it illustrates the potential legal constraints facing some governments who would engage in web censorship. On one level, sovereign states may censor what they like. However, if they wish to uphold international agreements they have made or maintain their status in a federation such as the EU, their attempts at web censorship may face legal constraints. Due to such prior commitments, the practical ability of liberal democratic states to censor the web is a function of both technical and legal factors.

WSSC:
webscience.org/2010/E.5.3 Digital crime
webscience.org/2010/E.5.4 Laws for Web access
webscience.org/2010/E.6.2.7 Web Censorship

Shklovski, I., 2011. Online Contribution Practices in Countries that Engage in Internet

Blocking and Censorship. *Human Factors*, pp.1109-1118.

This paper looks at how web users contribute online in the context of relatively high state censorship of the web. The authors note that much of the research on why and how people contribute online is focused on countries with strong legal protection of speech and ideas. The evidence gathered appears to confirm that online contribution in the face of heavy censorship has some significant differences.

This study, which is based on interviews and focus groups, has a number of methodological problems that undermine its external validity. Because of the risks associated with revealing one's online behaviours in a country which censors the web, not only have the participants been anonymised (as standard), but the country the sample is seeded from has also not been identified. While the authors do describe certain characteristics of the country (it is a 'digitally nascent state' with 30% internet penetration) the reader is left wondering what kind of population the results can be generalised to. Further, in recruiting participants, the researchers relied on personal contacts or encounters in internet cafes and public spaces, and 'snowball' sampling (participants recruited their friends and family) so the study may suffer from selection bias. These shortcomings may well be inevitable due to the nature of the study. Given the importance of upholding anonymity for citizens under certain regimes, and given the potential for rich qualitative data to reveal individual identities, similar studies are likely to face similar problems.

Despite these problems, this study provides a number of important insights. The section on strategies to deal with/handle blocking is particularly relevant. The effectiveness of web censorship depends partly on how citizens respond to it. While some participants described engaging in self-censorship, others employ a range of circumvention methods. Those with technical savvy used proxy servers and anonymisers to access and contribute to blocked content and platforms. Those without relied on social ties to exchange blocked content via email or social networking. Thus, even those without technical savvy may be able to thwart censorship attempts as long as at least one person in their network has social ties with someone who does know how to use circumvention tools.

WSSC:
webscience.org/2010/E.5.3 Digital crime
webscience.org/2010/E.5.4 Laws for Web access
webscience.org/2010/E.2.7 Virtual communities, groups and identity
webscience.org/2010/E.2.1 Social networks
webscience.org/2010/E.6.2.7 Web Censorship

Roberts, H. et al., 2010. *2010 Circumvention Tool Usage Report*. Beckman Center for Internet & Society at Harvard University

This is a study of the usage of three kinds of circumvention tools, which the authors identify as blocking resistant tools, simple web proxies and virtual private network (VPN) services. The authors use three research methods - a survey of 134 respondents self-reporting the usage statistics for their circumvention tool or service; analysing data of web site visits via GoogleAdPlanner; analysing data on search term frequency via Google Insights. Again, like Shklovski 2011, this paper illustrates the inherent difficulties in researching circumvention behaviours. The very purpose of such tools is to obscure evidence of web traffic, so attempts to monitor their use via web analytics will always be flawed.

Nevertheless, this is an important area of research. The mere existence of circumvention tools is not enough to prevent web censorship. Unless they are widely *used* in the general population, they may not have a significant countervailing effect on web censorship. The authors estimate that no more than 3% of Internet users in countries that engage in substantial filtering use circumvention tools. Most use simple web proxies rather than more sophisticated tools. Most users attempting to circumvent censorship search for generic terms like 'proxy' which return unsophisticated tools.

WSSC:
webscience.org/2010/C.3.6 Web Services
webscience.org/2010/E.5.3 Digital crime
webscience.org/2010/E.5.4 Laws for Web access
webscience.org/2010/E.2.7 Virtual communities, groups and identity
webscience.org/2010/E.6.2.7 Web Censorship

Diamond, L., 2010. Liberation Technology. *Journal of Democracy*, 21(3), pp.69-83.

This paper is a broad overview of issues to do with modern communication technologies and political empowerment and freedom, from a political science and sociology perspective. The author defines 'Liberation Technology' as 'any form of information and communication technology (ICT) that can expand political, social and economic freedom'. Censorship of the web is contextualised as part of a 'technological race' between 'democrats seeking to circumvent internet censorship and dictatorships that want to extend and refine it'.

While the arguments in this paper are important in highlighting the pervasiveness of web censorship in countries like China, they appear to imply that *any* increase or decrease in censorship is a function of political struggle between democratic and authoritarian governments. This approach is problematic for two reasons. First, it neglects the importance of technology. Second, it neglects the fact that, as the other papers here show, web censorship is not limited to authoritarian regimes, and is applied to a wide variety of content for different reasons, including security, morality and culture as well as politics.

WSSC:
webscience.org/2010/E.5.3 Digital crime
webscience.org/2010/E.5.4 Laws for Web access
webscience.org/2010/E.2.7 Virtual communities, groups and identity
webscience.org/2010/E.2.1 Social networks
webscience.org/2010/E.6.2.7 Web Censorship

Bambauer, Derek E., 2009. Cybersieves *Duke Law Journal*, Vol. 59, 2009; Brooklyn Law School, Legal Studies Paper No. 149.

This paper outlines a method for assessing web censorship decisions. The author argues that too much of the literature on censorship is value-based, and focused on a narrow context. Whether it is censorship of political material in non-democratic countries, censorship of child pornography in democratic countries, or takedown of copyright-infringing material, certain key principles such as openness, transparency, narrowness and accountability must be addressed. Here, the author focuses on the process by which censorship decisions are made. Whilst this paper does not directly address the key factors identified in the introduction (legal, technical, and social), it is important for anyone researching this area in so far as it encourages a value-neutral assessment of censorship in all its forms.

WSSC:
webscience.org/2010/E.5.1 Intellectual Property in the Web
webscience.org/2010/E.5.4 Laws for Web access

webscience.org/2010/E.6.2.7 Web Censorship

Dainotti, A. et al., 2011. Analysis of Country-wide Internet Outages Caused by Censorship. ***Proceedings of the 11th Usenix/ACM Internet Measurement Conference (IMC), Berlin, Germany, November 2011.***

This paper provides an overview of recent country-wide censorship-motivated internet outages in Egypt and Libya, and a method for monitoring this kind of web censorship. The research is timely, offering insights into a very recent phenomenon. While a number of other recent papers mention internet-wide outages, few develop the kind of methodological tools provided here to investigate them in detail.

A range of sources of large scale data were used, all of which were already accessible to academic researchers. These were analysed to reveal what the authors believe to be attempts by the Libyan government to test firewall-based blocking before resorting to BGP (Border Gateway Patrol) based internet outage. They propose that this method could be used to detect future outages and and similar macroscopically disruptive events in other regions.

WSSC:
webscience.org/2010/D.1 General Web Analysis
webscience.org/2010/D.2.1 Web data sampling and analytics
webscience.org/2010/D.2.4 Statistical Analysis of the Web
webscience.org/2010/E.6.2.7 Web Censorship

Michael Bailey and Craig Labovitz, 2011. Censorship and Co-option of the Internet Infrastructure. ***Technical Report CSE-TR-572-11*****, University of Michigan, Ann Arbor, MI, USA,**

This paper focuses on what the authors term 'infrastructure-based efforts to disrupt internet communication'. By this they mean censorship techniques which exploit weaknesses in the Internet’s underlying routing, naming and transport protocols. They draw together a variety of research to argue that there is a trend towards co-option and outright corruption of the internet infrastructure which threatens the long term future of the internet.

The authors briefly touch on the idea that governments cannot completely cut off the internet without hurting their economic interests with the rest of the world; a digital version of the 'Dictators Dilemma' (Francisco 2005). For instance, they note how in Iran, the ISP which served the stock exchange continued to operate through the general outage, and how in Egypt the communications infrastructure was running again within a week. This suggests some economic limits to this rather extreme form of web censorship (or at least trade-offs to be made).

There is also a brief outline of some of the challenges in detecting censorship. First, it is nearly impossible to track changes in populations who may be targeted by web censorship efforts, given the 4 billion possible IPv4 addresses (and more after IPv6). Second, it can be hard to establish whether lack of access is due to censorship efforts or merely natural disasters or cable cuts, etc.

WSSC:
webscience.org/2010/D.1 General Web Analysis
webscience.org/2010/D.2.1 Web data sampling and analytics
webscience.org/2010/D.2.4 Statistical Analysis of the Web

webscience.org/2010/E.5.4 Laws for Web access
webscience.org/2010/E.6.2.7 Web Censorship

Edman, M. & Ulent, B., 2009. On Anonymity in an Electronic Society : ***ACM Comput. Surv.*** **, 42(1), Article 5.**

This is a comprehensive survey of research done to design, develop and deploy systems for enabling private and anonymous communication on the internet – a key factor in web censorship circumvention. The authors review the major technologies in the field, their main flaws, and the future of online anonymous systems.

The authors suggest that a “many access points” approach to anonymous networks is the best way to circumvent censors. Under such a system, an individual attempting to circumvent domestic blocking only needs to find a single unblocked access point. Such access points, which can be operated by volunteers in uncensored countries, allow access to a larger network. The Tor network employs a *bridge relay* design, a version of this system. The authors also argue that *usability* and *incentives* are key to increasing the widespread uptake of any anonymity system – and a large, diverse user base is necessary to increase security.

webscience.org/2010/C.3.6 Web Services
webscience.org/2010/E.2.4 Peer production
webscience.org/2010/E.6.2.7 Web Censorship

Danezis, G. & Anderson, R., 2005. The economics of resisting censorship. ***Security & Privacy, IEEE*****, 3(1), pp.45–50.**

Peer to peer systems have evolved partly in response to censorship. In this paper, the authors (who have backgrounds in Computer Science and Security Economics) offer a model to assess the security of two types of peer-to-peer systems, based on economic analysis and conflict theory. One strategy to resist censorship in a peer-to-peer network is to distribute files (including the censored material) randomly across nodes in the network. This increases the costs for the censor of tracking down the files, and inconveniences everyone in the network – even those who have no interest in the material. Thus the *random model* appears to be naturally censorship-resistant. However, the authors argue that a *discretionary model* – in which individual nodes host only the content they wish to – will be better at resisting censorship.

This paper exhibits a promising multidisciplinary approach to assessing the effectiveness of web censorship resistance tools. It should be noted that while peer-to-peer systems are not *necessarily* web-based or used to access web content, they often are used this way and are therefore relevant to the question of how effective web censorship can be.

webscience.org/2010/C.3.6 Web Services
webscience.org/2010/D.2.6 Mathematical methods for describing Web services
webscience.org/2010/E.1.1.3 Economics of security, privacy and trus
webscience.org/2010/E.2.4 Peer production
webscience.org/2010/E.6.2.7 Web Censorship

References:

Akdeniz, Y., 2010. To block or not to block : European approaches to content regulation , and implications for freedom of expression. *Computer Law & Security Review*, 26(3), pp.260-272.

Bailey, M., and Labovitz, C., 2011. Censorship and Co-option of the Internet Infrastructure. Technical Report CSE-TR-572-11, University of Michigan, Ann Arbor, MI, USA,

Bambauer, Derek E., 2008. Filtering in Oz: Australia's Foray into Internet Censorship (December 22, 2008). Brooklyn Law School, Legal Studies Paper No. 125.

Bambauer, Derek E., 2009. Cybersieves *Duke Law Journal*, Vol. 59, 2009; Brooklyn Law School, Legal Studies Paper No. 149.

Benmeziane, S., 2011. *Tor Network Limits.* International Conference on Network Computing and Information Security (NCIS), 2011

Burnett, S., Feamster, N. & Vempala, S., 2010. *Chipping Away at Censorship Firewalls with User-Generated Content.* USENIX Security'10 Proceedings of the 19th USENIX conference on Security USENIX

Deva , S., 2007. *Corporate Complicity in Internet Censorship in China: Who Cares for the Global Compact or the Global Online Freedom Act?*. George Washington International Law Review, Vol. 39, pp. 255-319.

Chen, T.M. & Wang, V., 2010. Web Filtering and Censoring. *Computer* March 2010, pp.94-97.

Welch, C., 2011. "Global Internet Freedom Policy: Evolution, Action, and Reaction," IEEE Internet Computing, vol. 15, no. 6, pp. 65-69, Nov./Dec. 2011

Dainotti, A. et al., 2011. Analysis of Country-wide Internet Outages Caused by Censorship. *Proceedings of the 11th Usenix/ACM Internet Measurement Conference (IMC), Berlin, Germany, November 2011.*

Danezis, G. & Anderson, R., 2005. The economics of resisting censorship. *Security & Privacy, IEEE*, 3(1), pp.45–50.

Diamond, L., 2010. Liberation Technology. *Journal of Democracy*, 21(3), pp.69-83.

Duffy, J., 2009. Toothless Tiger , Sleeping Dragon : Implied Freedoms , Internet Filters and the Growing Culture of Internet Censorship in Australia . *Information and Communications Technology Law*, 11(2002), pp.91-105.

Edman, M. & Ulent, B., 2009. On Anonymity in an Electronic Society : *ACM Comput. Surv.* , 42(1), Article 5.

Edwards, L. 2010. Content Filtering and the New Censorship, Fourth International Conference on Digital Society, 2010 pp.317-322

Francisco, R. A. 2005. "The Dictator's Dilemma." Pp. 58-81 in Repression and Mobilization, Christian Davenport, Hank Johnston, and Carol Mueller, eds. Minneapolis: University of Minnesota Press.

Hamade, S., 2008. Internet Filtering and Censorship, itng, Fifth International Conference on Information Technology: New Generations 2008 pp.1081-1086, Karlin, J. & Forrest, S., 2009. Nation-state routing: Censorship, wiretapping, and BGP. *Arxiv preprint arXiv:0903.3218*.

Koumartzis, N. & Veglis, A., 2011. On the Pursue for a Fair Internet Regulation System A blueprint for a content blocking system encouraging participation by the Internet users. *Law & Policy*, pp.789-791.

Øverlier, L. & Syverson, P., 2006. Locating Hidden Servers. *IEEE Symposium on Security and Privacy, 2006*

Roberts, H. et al., 2010. *2010 Circumvention Tool Usage Report*. Beckman Center for Internet & Society at Harvard University

Roberts, H., Zuckerman, E. & Palfrey, J., 2011. *Circumvention Tool Evaluation.* Berkman Center for Internet & Society at Harvard University

Rosenberg, R.S., 2001. Controlling access to the Internet : The role of filtering. *Ethics and Information Technology*, 4, pp.35-54.

Stol, W.P. et al., 2009. Governmental filtering of websites: The Dutch case. *Computer Law & Security Review*, 25(3), pp.251-262.

Shoufeng C., Longtao H., Zhongxian L., Yixian Y., 2009. SkyF2F : Censorship Resistant via Skype Overlay Network. , *WASE International Conference on Information Engineering 2009* pp.350-354.

Wendy Seltzer, 2011. "Exposing the Flaws of Censorship by Domain Name," *IEEE Security and Privacy*, vol. 9, no. 1, pp. 83-87, Jan./Feb. 2011

Yarochkin, F.V. et al., 2008. Towards Adaptive Covert Communication System. *14Th IEEE Pacific Rim International Symposium on Dependable Computing*, pp.153-159.

Zittrain, J. & Edelman, B., 2003. Internet Filtering in China. *Internet Computing, IEEE* Volume 7 Issue 3, pp 70-77