Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control'[1]

Ben Wagner, Ludwig-Maximilians-Universität München and Universiteit Leiden

Introduction*

The academic debate on deep packet inspection (DPI) centres on methods of network management and copyright protection and is directly linked to a wider debate on freedom of speech on the Internet. The debate is deeply rooted in an Anglo-Saxon perspective of the Internet and is frequently depicted as a titanic struggle for the right to fundamentally free and unfettered access to the Internet.[2]

This debate is to a great extent defined by commercial interests. These interests whether of copyright owners, Internet service providers,

---

[1] (Bendrath 2009)

* A first draft of this paper was presented at the 3rd Annual Giganet Symposium in December 2008 in Hyderabad, India. For their advice and support preparing this paper I would like to thank: Ralf Bendrath, Claus Wimmer, Geert Lovink, Manuel Kripp, Hermann Thoene, Paul Sterzel, David Herzog, Rainer Hülsse, Wolfgang Fänderl and Stefan Scholz.

[2] (Frieden 2008, 633-676; Goodin 2008; Lehr et al. 2007; Mueller 2007, 18; Zittrain 2008)

application developers or consumers, are all essentially economic. All of these groups have little commercial interest in restricting free speech as such. However some might well be prepared to accept a certain amount of 'collateral damage' to internet free speech in exchange for higher revenues.

It can be argued that more transparent and open practices from network service providers are needed regarding filtering policy and the technology used. Nevertheless these practises are unlikely to fundamentally endanger free speech. Within the international system however, there are a large number of actors who have a considerable interest in limiting free speech, most obviously states.

As this paper will argue, the link between deep packet inspection and internet censorship is of far greater concern for freedom of speech than its use in traffic shaping or preventing copyright infringement. At the present time many of the states censoring the internet are already known to use deep packet filtering.[3]

A further question that arises in this context is whether state actors which censor the internet are following the lead of non-state actors and modifying content within the data stream rather than just blocking it. As DPI opens the door for far more subtle censorship methods, it could lead to a move from filtering internet content to editing it.

This paper will start by providing a short overview of DPI and it's technical capabilities, before discussing the motivations of state and non-state actors using DPI. A short sample of various actors using DPI for censorship purposes will be provided and various scenarios related to censorship which are enabled by DPI will be introduced. Finally, some preliminary conclusions will be drawn and technical and institutional responses to dpi will be sketched.

---

[3] For further examples see page 6

A short overview of deep packet inspection (DPI)

Deep packet inspection technology has been used in various forms since the late 1990s. Its initial development was closely linked to the security industry and early versions of DPI found their way into firewalls and other security software during this time.[4]

The rise of denial of service (DoS) attacks at the beginning of the 21st century further contributed to the rollout of DPI technology, as it was seen as an effective form of defence against this and other forms of attack.[5] Advances both in processing power[6] and in DPI technology allowed for the advent of security products including very advanced features such as "application intelligence."[7]

> "Generally speaking, DPI focuses on analyzing all the content of data packets passing through the network, the headers and the data protocol structures (as opposed to the prior "Shallow Packet Inspection" that would only analyze the packet header) and compares this content against rules or signatures (for example, virus signatures)."[8]

What Security Focus described as the "Firewall Evolution" in 2003 has quickly come to signify that a large number of security products and firewalls now incorporate DPI technology.[9] The use of DPI solutions has become so widespread that it is now used by many major global internet service providers. Furthermore, the use of DPI technology has

---

4 (Theta Networks Inc 2008; Top Layer Networks 2008)

5 (Houle and Weaver 2001, 21; Top Layer Networks 2008)

6 (Cox 2008)

7 (Leyden 2003)

8 (Theta Networks Inc 2008)

9 (Dubrawsky 2003-07-29)

become pervasive across the Internet, with most users frequently completely unaware of its existence.[10]

Before discussing the implications of the widespread use of DPI, a detailed description of the technical capabilities of DPI will be provided.

Technical capabilities of DPI technology

In its essence, what makes DPI different from 'traditional' ('shallow packet') filtering technology the capability to analyse all layers of the data packets sent across the Internet. This is frequently described as "drilling down" or "opening up the payload" to determine the actual content of the packet.[11]

Using a more traditional model, DPI technology could be compared to an automated system within the postal service, which opens each letter, checks the contents of the letter and modifies it as necessary, reseals the letter and then sends it on it's way. This process is completely transparent for both sender and recipient and because the process takes place without any perceivable delay both sender and recipient are unlikely to notice any difference.

What differentiates DPI filtering technology from previous forms of filtering is the precision and granular nature of the filters as well as the sheer scale of traffic that can be filtered.[12] While a less advanced filter such as a firewall would normally filter by IP-Address, host name or port of host and/or guest, DPI filtering technology is able to filter

---

[10] (Anderson 2008; Kassner 2008)

[11] (Anderson 2007)

[12] The signature mechanism in particular allows extremely precise rule sets which can be applied across internet traffic spectrum.

the entire packet based on keywords (i.e. the content of a website or email), the length and size of the packet as well as various behavioural and heuristic properties.[13]

When a packet is positively identified as matching a signature (a specific mixture of all of the above criteria) a wide variety of actions can be triggered. The most obvious example is to block the packet or disturb the entire internet connection. But simply removing the offending words, sentences or paragraphs is also possible, as is inserting other content into the packet or modifying large parts of it.

This allows DPI technology to scan packets and apply rules to them in a far more precise and effective manner. In turn, this extremely granular filtering mechanism allows for far more subtle and effective censorship.

Reasons for using DPI technology

The actors using DPI can be broadly split into state and non-state actors. Generally speaking, non-state actors using DPI technology normally run large networks and see DPI as part of their network management.

There are a wide variety of reasons for non-state actors to use DPI technology. Some of the most important are listed here[14]:

- Compliance with local government regulations by allowing the local governments access to the data flowing through their network (i.e. CALEA, RIPA)
- Security of the network by allowing non-state actors to monitor

[13] (Allot Communications 2007)

[14] The following lists are drawn from these sources: (Anderson 2007; Dawson 2008; Kassner 2008)

network packets for threats such as viruses or malware and filter these out as necessary

- Enforcement of network rules and legal decisions which can range from the bandwidth quotas to ensuring employee productivity to preventing illegal access to copyrighted content
- Management of the network; DPI helps ensure that all users are able to access the services they require and the administrators of the network are able to gain a very clear picture of the traffic flows within their network
- Service Differentiation allowing the network provider to provide highly granular levels of service to network users.
- Behavioural Advertising using DPI to create profiles of network users which can later be monetized through targeted advertising

State actors lack commercial interests in DPI technology and consequently are primarily interested in DPI for security reasons.

- Surveillance is one of the most obvious uses for DPI. As all layers of the packet are analysed in deep packet inspection, both the connection details and content of network communication can be analysed in great detail.
- Censorship of the Internet through content filtering can be more easily and effectively applied through the use of DPI technology.

To sum up these lists of preferences, the primary interests of non-

state actors are in the use of DPI for commercial reasons.[15] For state actors on the other hand the use of DPI is primarily of interest for security reasons. [16]

It is interesting to note that there is some convergence of interests between state and non-state actors. The commercial interests of non-state actors are not necessarily at odds with the security interests of state actors and as a result there is a certain amount of collaboration between the two groups. In the following sections of this paper, the use of DPI technology by state actors to enable censorship will be discussed in greater detail.

Actors currently using DPI for censorship

It is beyond the scope of this paper to provide an exhaustive list of all countries that are currently using DPI for censorship purposes.[17] Furthermore, due to the sensitive nature of Internet censorship, which is generally considered a security issue by state actors, it is difficult to draw up a definitive list of states. Access to information about

---

[15] The debate on DPI is part of a wider debate on network neutrality. As has been previously noted by Viviane Reding (EU Commissioner for Information Society & Media) this debate is primarily rooted in commercial interests:

> "A cynical observer may note that in the end this whole Net Neutrality debate is about hard cash. […] That it is about trying to use regulation as a means to get a better position around the negotiation table. That this is just about arm wrestling between big network providers and successful providers of internet services". (Orlowski, 2008)

[16] This is a simplified model of state and non-state actors, which was created for explanatory purposes in this paper. While it is reasonable to suggest that commercial and security aspects are perhaps the most important reasons for state and non-state actors respectively to use DPI, a more multifaceted and complete analysis of their actions would be necessary to fully understand motives.

[17] For an extended list of countries who engage in censorship, the most definitive list can be found at www.opennet.org. For more information about DPI usage in different countries, please check Ralf Bendrath's Deep Packet Inspection Project at Delft University: http://bendrath.blogspot.com/2008/04/deep-packet-inspection-or-end-of-net-as.html

censorship is frequently restricted and debates regarding Internet censorship are frequently securitized.[18]

This paper will concentrate on a select few countries, mainly because their use of DPI technology for the purpose censorship is well known. These are China and Tunisia.[19]

China is considered to be at the forefront of online censorship and operates some of the "largest and most sophisticated filtering systems in the world."[20] It employs a large variety of methods including the blocking of IP Addresses and keyword filtering of TCP traffic.[21]

The method used by China for keyword filtering is a form of deep packet inspection. TCP packets, which pass through the filter are scanned looking for specific keywords. If one of these keywords is found then the filtering system sends out TCP reset packets, which attempt to terminate the users connection at both ends.[22] As this behaviour is almost identical on all ISPs within China, the only reasonable conclusion is that China uses DPI technology nationally in order to filter internet content.

Beyond the very large and well-known example of internet censorship in China, Tunisia is another prime example of a country using deep packet inspection for the purpose of censorship. Indeed it is the case that an explosion in internet usage in Tunisia has been closely followed by a massive expansion of internet censorship.[23]

---

[18] (Buzan, Waever, and Wilde 1998)

[19] What has not been explored in this paper at all, but which warrants far more scholarly investigation, is why some states censor their Internet networks more, other states less and very few do not censor their Internet networks at all.

[20] (Zittrain, Palfrey, and OpenNet Initiative. 2005)

[21] (Zittrain and Edelman 2003, 70-77)

[22] (Clayton, Murdoch, and Watson 2006, 20-35)

[23] (OpenNet Initiative November 2005)

Tunisia uses DNS poisoning, IP blocking, Email censoring and a variety of other techniques to censor internet content. A recent report from Sami Ben Gharbia of Global Voices Advocacy indicates that deep packet inspection is being used in Tunisia to monitor and censor HTTP traffic.[24] Although it is unknown whether the use of DPI technology is widespread in Tunisia, it is likely that some forms of DPI technology for surveillance and filtering are currently in place.

Scenarios enabled by DPI technology

As has been previously suggested in this paper, DPI technology is sufficiently powerful to not only to filter content buy also to modify it. While there is as of today no evidence that packet modification has taken place for censorship purposes, it is clear that this procedure has been used for behavioural advertising in both the United States and the United Kingdom.[25]

A report prepared on DPI usage by NebuAd in the USA notes that the "advertising hardware monitors, intercepts and modifies the contents of Internet packets"[26]. DPI technology is used to scan packages and then "inserts code by impersonating the end-point server and adding JavaScript". This example clearly shows the technically ability of DPI technology to modify the payload of Internet traffic. However this specific usage of DPI reflects the commercial interests of non-state actors.

In this context it is plausible to suggest that state actors are following the lead of non-state actors in modifying Internet content. To take the

---

[24] (FREEDOM AGAINST CENSORSHIP THAILAND 22-09-08; Gharbia 2008)

[25] (Metz 2008; Morelli 2007)

[26] (Topolski 2008)

example of a HTTP request to the website bbc.co.uk from an internet user in China: at present all packets attempting to access BBC.co.uk are blocked.[27] This is a blunt but effective method of ensuring that the content is censored for internet users in China, but a fairly obvious method that is prone to circumvention (the user is most likely aware that bbc.co.uk exists and may attempt to access it through other means).

Using DPI technology, the censorship regime in China has the ability to modify any packets running through its network. It could plausibly create a signature for pages on bbc.co.uk, which contain opinions it considers censorable and use DPI to rewrite these pages as they pass through the network. This would ensure that the content is appropriately sanitized by the time it arrives on a Chinese Users Screen. Both inserting several lines below a BBC news article or removing several of the most critical parts of an article would be a far more effective form of censorship than blocking bbc.co.uk as a whole.

Any such modifications would only be visible within China and could equally be configured to only take effect in certain parts of the country. This form of extremely subtle filtering and modification as the packets pass through the network would be extremely difficult to pinpoint and would also make it extremely difficult to distinguish between the original and the censored Chinese version.

To return to the analogy of the post office, this form of censorship is akin to all copies of “The New York Times,” (for lack of a BBC print publication) which are sent to China being opened, meticulously censored and rewritten in a manner completely transparent for any newspaper reader, resealed and sent on without any perceivable delay.

---

[27] Although some parts of BBC.co.uk have been unblocked recently, it remains unclear how much of the site can be viewed.

Needless to say a 'virtual edit button' for all Internet pages viewed in China is an equally powerful and concerning development.[28] But this is precisely what DPI technology currently allows. Although there is at present no evidence that DPI technology is being used to this effect, such subtle and advanced filtering techniques are likely to become more common, as DPI continues to spread through the network.

Many of the countries which are the most prolific censors, also to go to some lengths to mask their use of censorship.[29] Using DPI not only to filter but also modify Internet content is a logical continuation of previous censorship practises. Furthermore as awareness of the potential for such modification is very low, content providers have no mechanisms in place to prevent censorship of this kind.

Preliminary Conclusions

As there is no significant divergence of interests between state and non-state actors, DPI technology will continue to spread throughout global Internet networks. This spread of DPI technology effectively provides the necessary foundations for the use of DPI as a censorship technology.

While it has not been discussed in this paper, it should also be noted that a wide variety of state actors use DPI technology for surveillance

---

[28] "Concerning" here – as in the introduction – is in relation to freedom of speech. If free speech on the Internet is considered to be a value worth protecting, the development of powerful pervasive censorship technologies could be cause for concern.

[29] Of the all the countries listed as censoring the internet on http://opennet.net, there is a relatively strong correlation between high levels of censorship and low levels of transparency.

and espionage.[30] Depending on the technical means used, the same systems, which are used for content filtering, may also be used for surveillance purposes. Although there is little evidence for or against such dual uses in regards to DPI, dual uses of the same technical system for content filtering and surveillance have been known to exist.[31]

Despite the fact that deep packet inspection has been in use on the Internet for some time, it is now becoming widespread. There is still a great lack of awareness of the scale and capabilities of DPI on many levels, which has so far made meaningful policy debates about the technology difficult.

In regards to DPI and censorship, there is very little literature to be found on this subject at all. This seems to indicate that the full impact of DPI technology on censorship has yet to be debated. The main response to the use of DPI technology in Western societies so far has been the Network Neutrality debate.

It is probably fair to say that a concept like network neutrality could go a long way to preventing censorship via DPI. However as there is currently no agreed definition of what network neutrality is or could be and the distant idea of network neutrality as a 'global norm' is still some way off.[32]

As one of the more measured contributors to the network neutrality debate has noted, "the strongest opposition [to Network Neutrality] is likely to come from [...] and from national governments or third

---

[30] (United States. Congress. House. Committee on Homeland Security. Subcommittee on Economic Security, Infrastructure Protection,and Cybersecurity. and United States. Congress. House. Committee on Homeland Security. Subcommittee on Emergency Preparedness, Science,and Technology. 2007)

[31] (Villeneuve 2008, 16)

[32] (Mueller 2007, 18)

parties attempting to maintain their power to filter and censor the Internet."[33]

Beyond institutional solutions such as network neutrality as a global norm, the means in which content can be technically protected from DPI should also be considered. At present there is a general lack of awareness regarding the ability of third parties to edit content as it travels through the network, but as awareness of this grows technical means of preventing deep packet inspection are likely to become more common.

The two most common technical measures which are able to prevent deep packet inspection are encryption technology and non-textual frameworks.[34] Whether their use will spread in response to the increased usage of DPI remains to be seen.

It is likely that the growing use of DPI within networks will have a significant impact on the development of the internet as a whole.[35] Censorship is one of the most fundamental facts of the Internet in large parts of the world and is likely to be influenced by the spread of DPI.

Although network neutrality as a global norm is still some way off, a more open public policy debate might help define a framework in which an essentially generic technology such as DPI can be used without endangering freedom of speech or encouraging censorship.

---

[33] ibid. p. 16

[34] (Lehr et al. 2007; Wolfgarten 2006, 1–10; Wachter 2008)

[35] (Zittrain 2008)

References

Allot Communications. Digging deeper into deep packet inspection (DPI). 2007 [cited 10/6/2008 2008]. Available from https://www.dpacket.org/articles/digging-deeper-deep-packet-inspection-dpi (accessed 10/6/2008).

Anderson, Nate. Deep packet inspection under assault over privacy concerns. 2008 [cited 10/3/2008 2008]. Available from http://arstechnica.com/news.ars/post/20080512-deep-packet-inspection-under-assault-from-canadian-critics.html (accessed 10/3/2008).

Anderson, Nate. Deep packet inspection meets 'net neutrality, CALEA'. 2007 [cited 10/3/2008 2008]. Available from http://arstechnica.com/articles/culture/deep-packet-inspection-meets-net-neutrality.ars (accessed 10/3/2008).

Anderson, Ross J. 2008. Security engineering : A guide to building dependable distributed systems. Indianapolis, Ind.: Wiley.

Bendrath, Ralf. DPI as an Integrated Technology of Control – Potential and Reality. 2009. Available from http://dpi.priv.gc.ca/index.php/essays/dpi-as-an-integrated-technology-of-control-%E2%80%93-potential-and-reality/ (accessed 23/6/2009).

Briscoe, B. 2007. Flow rate fairness: Dismantling a religion. COMPUTER COMMUNICATION REVIEW 37, (2): 63-74.

Buzan, Barry, Ole Waever , and Jaap de Wilde. 1998. Security : A new framework for analysis. Boulder, Colo.: Lynne Rienner Pub.

Center for Democracy and Technology. Online behavioral advertising: Discussing the ISP-ad network model. 2008 [cited 10/06/2008 2008]. Available from http://www.cdt.org/publications/policyposts/2008/15 (accessed 06/10/2008).

Clayton, R., S. J. Murdoch, and R. N. M. Watson. 2006. Ignoring the great firewall of china. Lecture Notes in Computer Science.(4258): 20-35.

Computer & Communications Industry Association. OPEN INTERNET/NEUTRAL BROADBAND ACCESS. 2008 [cited 10/06/2008 2008]. Available from http://www.ccianet.org/docs/abstracts/2008/OpenInternet2008.pdf.

Cooper, Alissa. What your broadband provider knows about your web use: Deep packet inspection and communications laws and policies. in CENTER FOR DEMOCRACY & TECHNOLOGY [database online]. 2008 [cited 10/06/2008 2008]. Available from http://cdt.org/testimony/20080717cooper.pdf.

Cox, Dennis. Deep packet inspection and the role of network processors. 2008 [cited 10/6/2008 2008]. Available from https://www.dpacket.org/blog/dennis/deep-packet-inspection-and-role-network-processors (accessed 10/6/2008).

Dawson, Travis. What does deep packet inspection mean to you? 2008 [cited 10/6/2008 2008]. Available from https://www.dpacket.org/articles/what-does-deep-packet-inspection-mean-you (accessed 10/6/2008).

Dubrawsky, Ido. Firewall evolution - deep packet inspection. 2003-07-29 [cited 10/3/2008 2008]. Available from http://www.securityfocus.com/infocus/1716 (accessed 10/3/2008).

FREEDOM AGAINST CENSORSHIP THAILAND. Tunisia: Silencing online speech-global voices « FACT - freedom against censorship thailand. 22-09-08 [cited 10/6/2008 2008]. Available from http://facthai.wordpress.com/2008/09/22/tunisia-silencing-online-speech-global-voices/ (accessed 10/6/2008).

Frieden, R. 2008. Internet packet sniffing and its impact on the network neutrality debate and the balance of power between intellectual property creators and consumers. Fordham Intellectual Property, Media & Entertainment Law Journal. 18, (3): 633-76.

Gharbia, Sami B. Global voices advocacy » silencing online speech in tunisia. 2008 [cited 10/6/2008 2008]. Available from http://advocacy.globalvoicesonline.org/2008/08/20/silencing-online-speech-in-tunisia/ (accessed 10/6/2008).

Goodin, Dan. Ad hoc malware police besiege net neutrality: When does crime fighting become censorship? 2008 [cited 10/6/2008 2008]. Available from http://www.theregister.co.uk/2008/09/15/online_crime_vs_censorship/print.html (accessed 10/6/2008).

Hamade, S. N. 2008. Internet filtering and censorship. Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on: 1081.

Houle, Kevin J., and Weaver, George M. Trends in denial of service attack technology. in CERT® Coordination Center [database online]. 2001 [cited 10/3/2008 2008]. Available from http://www.cert.org/archive/pdf/DoS_trends.pdf (accessed 10/3/2008).

Kassner, Michael. Deep packet inspection: What you need to know. 2008 [cited 10/3/2008 2008]. Available from http://blogs.techrepublic.com.com/networking/?p=609 (accessed 10/3/2008).

Lehr, William H., Marvin A. Sirbu, Sharon E. Gillett, and Jon M. Peha. 2007. Scenarios for the network neutrality arms race. 2007.

Leyden, John. Don't put app protection on your firewall, mr jones. 2003 [cited 10/3/2008 2008]. Available from http://www.theregister.co.uk/2003/11/13/dont_put_app_protection/print.html (accessed 10/3/2008).

Marsden, Christopher. 2008. Beyond europe: The internet, regulation, and multistakeholder governance--representing the consumer interest? Journal of Consumer Policy 31, (1): 115-32.

Metz, Cade. Phorm secretly tracked americans too. 2008 [cited 10/6/2008 2008]. Available from http://www.theregister.co.uk/2008/08/13/phorm_us_tests/print.html (accessed 10/6/2008).

Morelli, Filippo. To own, to be owned, or what else? BT and its proxies. 2007 [cited 10/6/2008 2008]. Available from http://www.spikelab.org/blog/btProxyHorror.html (accessed 10/6/2008).

Mueller, Milton. Net neutrality as a global principle of internet governance. in Internet Governance Project [database online]. 2007 [cited 6/10 2008]. Available from http://www.internetgovernance.org/pdf/NetNeutralityGlobalPrinciple.pdf.

Ohm, Paul. 2008. The rise and fall of invasive ISP surveillanceSSRN.

OpenNet Initiative. Internet filtering in tunisia in 2005: A country study November 2005 [cited 10/6/2008 2008]. Available from http://opennet.net/sites/opennet.net/files/ONI_Tunisia_Country_Study.pdf (accessed 10/6/2008).

Orlowski, Andrew. Google's coup: The internet's first rule book. [cited 12/1/2008 2008]. Available from http://www.theregister.co.uk/2008/10/15/neutrality_in_europe_analysis/page3.html (accessed 12/1/2008).

Søraker, Johnny Hartz. 2008. Global freedom of expression within nontextual frameworks. The Information Society 24, (1): 40-6.

Theta Networks Inc. Deep packet inspection overview. 2008 [cited 10/3/2008 2008]. Available from http://www.thetanetworks.com/resources/deep_packet_inspection_overview.html (accessed 10/3/2008).

Top Layer Networks. Stop DoS attack - cyber attack - firewall solutions. 2008 [cited 10/3/2008 2008]. Available from http://www.toplayer.com/content/resource/faq.jsp (accessed 10/3/2008).

Topolski, Robert M. Network management and consumer expectations. April 17, 2008 [cited 10/6/2008 2008]. Available from http://www.freepress.net/files/FCC_testimony_Robert_Topolski_OpeningStatement_withnotes.pdf (accessed 10/6/2008).

Topolski, Robert M. NebuAd and partner ISPs: Wiretapping, forgery and browser hijacking

. 2008 [cited 10/6/2008 2008]. Available from http://www.publicknowledge.org/pdf/nebuad-report-20080618.pdf (accessed 10/6/2008).

Villeneuve, Nart. BREACHING TRUST: An analysis of surveillance and security practices on China's TOM-skype platform. in Information Warfare Monitor, ONI Asia [database online]. 2008 [cited 10/6/2008 2008]. Available from http://www.infowar-monitor.net/breachingtrust.pdf (accessed 10/6/2008).

Wachter, Christoph. How picidae works. 2008 [cited 10/10/2008 2008]. Available from http://www.picidae.net/how_picidae_works/ (accessed 10/10/2008).

Williams, Chris. Berners-lee backs web truthiness labelling scheme. 2008 [cited 10/6/2008 2008]. Available from http://www.theregister.co.uk/2008/09/15/berners_lee_foundation/print.html (accessed 10/6/2008).

Wolfgarten, Sebastian. 2006. Investigating large-scale internet content filtering. M.Sc. in Security & Forensic Computing., Dublin City University.

Zittrain, Jonathan. 2008. The future of the internet and how to stop it. New Haven [Conn.]: Yale University Press.

Zittrain, Jonathan, and Edelman, Benjamin. Documentation of internet filtering in saudi arabia. in Harvard Law School [database online]. Cambridge, Mass., 2002.

Zittrain, Jonathan, and B. Edelman. 2003. Internet filtering in china. IEEE INTERNET COMPUTING 7, (2): 70-7.

Zittrain, Jonathan, John G. Palfrey, and OpenNet Initiative. 2005. Internet filetring in china in 2004-2005 : A country study. Cambridge, Mass.: Berkman Center for Internet & Society.