Trends in transition from classical censorship to Internet censorship: selected country overviews

Constance Bitso, Ina Fourie and Theo J.D. Bothma

Constance Bitso
Department of Information Science, University of Pretoria, Lynnwood Road,
Pretoria, South Africa, 0002
Email: conniebitso@gmail.com

Ina Fourie
Department of Information Science, University of Pretoria, Lynnwood Road,
Pretoria, South Africa, 0002
Email: ina.fourie@up.ac.za

Theo J.D. Bothma
Department of Information Science, University of Pretoria, Lynnwood Road,
Pretoria, South Africa, 0002
Email: theo.bothma@up.ac.za

Abstract

Censorship is no longer limited to printed media and videos. Its impact is felt much more strongly with Internet related resources of information and communication such as access to websites, email and social networking tools which is further enhanced by ubiquitous access through mobile phones and tablets. Some countries are marked by severe restrictions and enforcement, a variety of initiatives in enforcing censorship (pervasive as well as implied), and initiatives to counter censorship. This article reflects on trends in Internet censorship in selected countries, namely Australia, Chile, China, Finland, Libya, Myanmar, Singapore, Turkey, and the United Kingdom (UK). Negative and positive trends are noted. Negative trends include those involving issues of Internet related privacy; ubiquitous society and control; trends in Internet related media being censored; trends in filtering and blocking Internet content *and blocking software; trends in technologies to monitor and identify citizens using the Internet to express their opinion and applying 'freedom of speech'; criminalization of legitimate expression on the Internet; trends in acts, regulations and legislation regarding the use of the Internet and trends in government models regarding Internet censorship; trends in new forms of Internet censorship; trends in support of Internet censorship; trends in enforcing regulations and Internet censorship; trends in Internet related communication surveillance. Positive trends include trends in reactions to Internet censorship; attempts and means to side-step Internet censorship; trends in cyber actions against Internet censorship; trends in innovative ways of showing opposition to Internet censorship.*

Introduction

Censorship has been around for many years. Traditional censorship has been associated with the removal of material from open access by any governing authority including removal of material from general use by any means solely for the purpose of restricting access to the ideas or information in the item (McDonald 1993:52). It has been explained as a moral or legislative process by which society agrees to limit what an individual can do, say, think, or see (Depken II 2006). All societies have forms of censorship, effective only with sufficient threat and severity of punishment for violating the censorship rule (Depken II 2006). Censorship encompasses all the processes whereby the dissemination of information, opinions or ideas are suppressed (Munro 1979:4), and is often associated with political control (Malley 1990:2).

The Internet brought numerous opportunities for people on a global scale to access all kinds of information and to raise levels of informedness, decision-making, education, and empowerment of citizens from all levels of society and in all contexts (e.g. politics, religion, health, education, social interaction). This is enhanced by the diversity of methods for Internet access ranging from traditional laptops and desktop networks to ubiquitous means of access through mobiles and tablets. Internet censorship can be intentional, unintentional, or implied due to other restrictions. An example of the latter would be people who are limited in using the Internet and its associated technologies (e.g. WWW, social media) due to reasons often associated with the digital divide, lack of Information Communication Technology (ICT) infrastructure and lack of skills such as computer, information and other digital skills.

To identify and understand trends in the transition from classical censorship to Internet censorship, this article briefly reflects on the background of traditional censorship, the clarification of key concepts, the literature on Internet censorship, the identification of trends to monitor, and the highlights noted from data mining for selected countries. The latter is considered essential if we intend to raise country specific awareness of the impact Internet censorship has on intellectual freedom and human rights.

Background on traditional censorship

Censorship has been part of human history for many years (Oboler 1980:80), and there is no evidence that it is likely to decrease (Robotham and Shields 1982: 58); in fact it seems to be increasing in some countries. Censorship came as the result of concerns raised by groups such as parents, teachers and the clergy as well as politicians, political candidates, law-enforcement officials, school administrators or board members, and trustees of various organisations (Robotham and Shields 1982:58). There are various reasons for traditional censorship: information is censored because of political, social, economic, religious, philosophical, moral, ideological, military, corporate, and educational reasons, and where people feel material offers an attack on themselves and their personal values (Oboler 1980).

Traditional censorship is evident in various contexts such as public libraries (Thompson 1975), school libraries (Oboler 1980), the press (Duke & Tamse 1987), theatre and religion (Hadfield 2001). It can take many forms, including voluntary censorship (McDonald 1993:5) such as when a librarian, as a result of real or anticipated pressure from school boards and communities, removes or restricts resources or does not purchase certain titles.

With the advent of the Internet, a new and more serious form of censorship developed – Internet censorship.

Clarification of terminology

Terminology used with regard to the Internet and censorship includes e-censorship, cyber censorship, Net censorship and Internet censorship (the concept preferred for this article).

Internet censorship builds on interpretations of traditional censorship. Wikipedia defines censorship as “the suppression of speech or other public communication which may be considered objectionable, harmful, sensitive, or inconvenient to the general body of people as determined by a government, media outlet, or other controlling body". Censorship of information on censorship is referred to as meta-censorship.

Background on internet censorship

As early as the 1990's when proliferation of the Internet started, countries were already enacting legislation on Internet censorship (Cohen 1997:12). The rationale was the desire to protect children, public morals, and public safety and to silence racists and hate speech. Often the real reason was promoting political objectives. Internet censorship increased since 1997 and was marked by disparities in policy, types of governance, divergent approaches in adherence to international human rights' treaties, restrictions on Internet access and content affected (Cohen 1997). Gradually Internet censorship has become more visible, gaining attention from scholars and research institutions in different disciplines including media and communication, information technology, law, political science, and economics. Reports on Internet censorship are also produced by advocacy groups such as the Paris-based Reporters without Borders and the Washington DC-based Freedom House (Al-Saqaf 2010).

Internet censorship is complex; it concerns the Internet's structure and application as well as Internet users' behaviour, state control, and the socio-economic and political situations of a country (Al-Saqaf 2010). A study of Internet censorship needs to consider the motivations for censorship, concerns for censorship weighed against the abundance of opportunities and benefits offered by the Internet, how it is implemented, who is taking responsibility, means for countering Internet censorship, etc. These issues are addressed in the brief literature review before moving to prominent trends that manifest and need to be monitored for individual countries.

Literature review on internet censorship

Formal, scholarly literature is marked by arguments, concerns, and steps taken regarding Internet censorship. There is a considerable difference between the number of publications appearing in the early years of the Internet and more recent publications (2008-2011) with early days' output being more prolific. Also, reports are on a limited number of countries only.

The Internet can act as a social, cultural, commercial, educational, and entertainment global communications system whose legitimate purpose is to benefit and empower people and lower barriers in access to information. It is the largest global, decentralized communication network with invisible boundaries (Akdeniz and Altiparmak 2008), and owned by nobody (Cohen 1997). It can enhance the exercising of human rights and fundamental freedoms, such as the right to freedom of expression, access to information, right to communication, and the right to assembly (Akdeniz and Altiparmak 2008). Any person can be empowered (Deibert and Rohozinski 2010), communicate instantly with a huge international audience (Cohen 1997), or publish (Akdeniz 2007). It is especially important in the academic world (Peace 2003) and in schools (Clyde 1997). While governments recognize that the benefits of the Internet far outweigh its negative aspects, they maintain that the negative aspects (discussed in the next section) cannot be ignored (Cohen 1997:13).

Concerns for Internet use that can be addressed by censorship

One of the major concerns of Internet use is the unlimited freedom to post information on the Web without a review process. Anyone can post a professional-looking website that contains biased, incorrect, or dangerous information (Colaric 2003). Therefore, there is serious concern especially when it comes to letting children use the Web, leading to motivations for censorship to protect children. Depken II (2006) notes a number of concerns of Internet use that led to censorship including pornography, hate speech, and bomb-making instructions. The justification for censorship of such content is that this would lead to a greater social good, even if individuals are limited in what they can consume on the Internet. There is also concern for the duplication of material on the Internet and copyright violations (Deibert 2003).

Censorship can be enforced by many stakeholders such as universities, schools, parents, and individual self-censorship. Governments are, however, the most important enforcers using various means of filtering (Deibert *et al*. 2008; 2010; 2012). Faris and Villeneuve (2008:7) note government Internet filtering against political transformation and information by opposition parties, political reform, legal reform, minority rights and ethnic content, as well as women's rights, hate speech, public health, minority faith, free e-mail, pornography, commercial sites, groups and social networking. Governments use legal frameworks on local, national and federal levels to enforce censorship (Malley 1990; Dahan *et al*. 1995; Cohen 1997; Deibert *et al*. 2008).

Censorship is also intertwined with social responsibility (Malley 1990: 21) involving parents, teachers, clergy, politicians, social groups, librarians (Truett 1997; Colaric 2003), hospital management (Bernstein 2004), users in content rating systems, and privatized censorship (Akdeniz 2008).

Arguments against and for censorship

As noted earlier the advantages of the Internet and the numerous opportunities offered, as well as the concerns for Internet content need to be noted. The challenge is to grab the opportunities and exploit them to the fullest, while containing, if not eliminating, the threats (Bihani and Hamilton 2009).

Supporters of censorship such as Cohen (1997) argue that information over the Internet is controlled because it carries a certain amount of potentially harmful or illegal content that can instigate criminal activities and terrorism. Johnson (1998) however argues for better training for children and students (rather than censorship) to prepare them to deal with such material. Supporters of censorship also express concerns for cybercrime such as viruses, spying, phishing and botnets (Bihani and Hamilton 2009). However, those that are against the issue indicate that the primary motivation for censorship is often political (Bailey and Labovitz 2011). They are concerned about the impact on intellectual freedom (Malley 1990), and that Internet censorship is often hidden (Karhula 2011). According to Gorman (2005) any sensible view of the Internet must admit that some sort of censorship or regulation is necessary, and this is put into practice differently by different societies and countries.

The rationale for Internet censorship differs from country to country. Cohen (1997) identified reasons common to many countries:

- National security (information on weapons' making, illegal drugs and protection from terrorism);
- Protection of minors (information on abuse, forms of marketing, violence and pornography);
- Protection of human dignity (incitement to racial hatred or discrimination);
- Economic security (fraud, pirating of credit cards);
- Information security (malicious hacking);
- Protection of privacy (protection against unauthorized communication of personalized data, electronic harassment, spamming);
- Protection of reputation (defamation, unlawful comparative advertising);
- Protection of intellectual property (the unauthorized distribution of works under copyright such as music, software, books, etc).

Means of counteracting Internet censorship

Al-Saqaf (2010) reveals some means to counteract Internet censorship. This includes allowing access to blocked websites by using overseas Web proxies (i.e. intermediate machines that retrieve Web pages on behalf of users for a number of purposes such as increased efficiency and privacy protection) (also noted by Feamster *et al*. 2002) and the use of proxies that are run by individual users on their home and office personal computers (PCs) anywhere in the world (Feamster *et al*. 2002). Dahan *et al*. (1995) note the use of anonymous remailers and encryption software tools that allow anonymous dissemination of information.

Internet censorship in specific countries as noted in scholarly literature

Censorship at varying levels is occurring in various countries. Discussions can be found in Gorman (2005) on China; Ang and Nadarajan (1996) on Singapore; Bambauer (2009b) on Australia; Wang (2003) on the United States of America; Editors of *Public Library Quarterly* (2008) on South Korea. More comprehensive country based censorship is revealed in studies by OpenNet Initiative Research in the books *Access denied*... (Deibert *et al*. 2008), *Access Controlled*… (Deibert *et al*. 2010) and *Access Contested*… (Deibert *et al*. 2012). Informative studies covering various countries were also done by Electronic Frontiers Australia (2002) and Warf (2011).

Warf (2011) classifies countries' censorship as:

- **Worst Internet censors** e.g. China, Burma/Myanmar, Vietnam and Iran.
- **Severe Internet censors** e.g. Russia, Belarus, Pakistan, Arab World countries such as Saudi Arabia, Jordan, Bahrain, etc.
- **Moderate Internet censors** e.g. Thailand, Malaysia, Singapore, Indonesia, India, Central Asia, United Arab Emirates, Sub Saharan Africa and Latin America.
- **Light Internet censors** e.g. Latin America countries, Southern and Eastern Europe.
- **Uncensored Internet** e.g. Western Europe and USA. (For the latter it might be that there are forms of implied censorship not noted.)

According to Deibert *et al*. (2010) Internet filtering, censorship of Web content and online surveillance are increasing in scale, scope, and sophistication around the world, in democratic countries as well as in authoritarian states. The first generation of Internet controls consisted largely of building firewalls at key Internet gateways; the 'Great Firewall of China' is considered one of the first national Internet filtering systems. The degree and reasons for censorship differs from country to country (Cohen 1997); so does the type of filtering ranging from pervasive filtering, substantial filtering, selective filtering, suspected filtering and no evidence of filtering (OpenNet Initiative 2004). Frechette (2005) alludes to over regulation and under regulation of the Internet. In some countries such as China, Internet censorship receives much attention in the mass media, while censorship in other countries, such as the United States of America does not feature much.

Bambauer (2009a) asks a pertinent question: how can we make normative distinctions among Saudi Arabia's decision to censor Internet pornography, China's efforts to suppress political dissent on-line, and America's moves to filter out illegal MP3 files from the Web? This is because censorship stems from different value judgments made by countries about the relative importance of free expression, protection of minority interests, concern for societal cohesion, and national security goals (Bambauer 2009a). Countries differ not only in their intent to limit access to material on-line, but in the content they ban, the precision of their blocking, and the voice they offer citizens in decision making (Bambauer 2009a).

Deibert *et al*. (2008; 2010; 2012) outline a summary of selected countries based on the OpenNet Initiative research. They explain that legal and regulatory frameworks, including Internet law, the state of Internet access and infrastructure, the level of economic development, and the quality of governance institutions, are central to determining which countries resort to filtering and how they choose to implement Internet content controls. They distinguish the following categories of filtering:

- **Political**: the focus is on websites that express views opposing governments. In most cases the content is related to human rights, freedom of expression, minority rights and religious movements.
- **Social**: the focus is on content related to sexuality, gambling, illegal drugs and alcohol and other issues considered illicit.
- **Conflict/security**: focuses on content related to armed conflicts, border disputes, and militant groups.
- **Internet tools**: websites that provide email, Internet hosting, search, translation, voice-over Internet Protocol, and telephone service, as well as circumvention methods.

China keeps the dissemination of information and freedom of expression to a minimum (Dickinson 1997). It operates the world's most extensive and sophisticated Internet censorship system, yet rarely admits it filters information (Bambauer 2009a). The Chinese filtering apparatus is multi-layered and users are not informed when they are prevented from reaching proscribed material; instead, their Internet connections are re-set, or their e-mail messages never reach their destinations (Bambauer 2009a).

Iran is associated with harsh controls and Internet censorship. According to Calingaert (2010), the government of Iran has restrictions on bandwidth by making uploads of photos and videos very slow. In addition, transmissions of text messages on mobile phones are also blocked on different occasions to disrupt protests. Government disruption of social networking sites such as Facebook impedes the ability of Iranians to share information and to organize protests. Government surveillance on Internet communications may also have contributed to the arrests of dissidents (Calingaert 2010).

Forms of Internet censorship

Emerging tools and techniques for Internet censorship go beyond mere denial of information**.** They aim to normalize (or even legalize) Internet control, and include targeted viruses and the strategically timed deployment of distributed denial-of-service (DDoS) attacks, surveillance at key points of the Internet's infrastructure, take-down notices, stringent terms of usage policies, and national information shaping strategies (Deibert *et al*. 2010). Measures of control also include Internet curfews (i.e. the Internet is down for a few hours) and Internet blackouts (i.e. when there is no Internet access for up to several days). Internet censorship is sometimes used as a 'weapon' to suppress the dissemination of information and to stifle dissent; it can be done through harassment of those who publish information online (i.e. through fear) (Grothoff *et al*. 2003). According to Zittrain and Palfrey (2008a: 2) Internet technical filtering is the "technical blockage of the free flow of information across the Internet". Zittrain and Palfrey (2008a) and Murdoch and Anderson (2008) explore the legal and social measures used in Internet censorship in some detail.

A comprehensive review of tools and technology for Internet filtering (including surveillance and non-technical censorship methods) is outlined by Murdoch and Anderson (2008). Filtering mechanisms include:

- **TCP/IP header filtering**: The censor's router can inspect the Internet Protocol [IP] address and port number of the destination. If the destination is found to be on a blacklist, the connection is dropped or redirected to a page indicating that access to the destination is denied.

- **TCP/IP content filtering**: The censor's router inspects the packet contents for any patterns or keywords that may be blacklisted. The focus is not on content, but on where packets are going to or coming from.
- **Domain Name Server (DNS) Tampering**: Normally, domain name servers are accessed by user computers to retrieve the corresponding IP address of a given domain. Through domain name server tampering, domain name resolution could fail as the router could send back an erroneous response that does not contain the right IP address; hence the connection fails.
- **Hyper Text Transfer Protocol (HTTP) Proxy Filtering**: In some cases users are forced to use HTTP proxies that are assigned for accessing the Internet. Those proxies may be the only way to reach the Internet and hence all traffic that goes through the proxies can be monitored. This is more powerful than TCP/IP headers and DNS filtering.
- **Hybrid TCP/IP and HTTP Proxy filtering**: Because using HTTP Proxy Filtering is often demanding, a solution was devised to use only HTTP Proxy filtering for a list of IP addresses known to have prohibited content. If any of those IP addresses is accessed, traffic is redirected to a transparent HTTP proxy, which inspects the transferred stream and filters any banned content.
- **Denial-of-Service (DoS) attacks:** Denial-of-service attacks can be launched on a host server. A large number of computers request services from a particular server overwhelming it with too much traffic and causing the server and its connection to stall.
- **Server takedown**: Through legal, extra-legal or pressure methods, a company hosting a specific server could take it down and disconnect it from the Internet. The owner of the server may be able to transfer the server's contents however – provided that a backup copy exists – to another hosting company within hours.
- **Surveillance**: Constant technical monitoring through logging transfers between the host and the Internet user. If banned content is found in the transferred stream, actions – legal or extra-legal – could be taken against the user, the host or both. Such acts could trigger a sense of fear, causing the host to refrain from publishing such content and causing the user to hesitate from accessing it.
- **Social techniques:** This includes the requirement to show photo identification (ID) before using public computers at libraries or Internet cafés; social or religious norms that force Internet users to avoid opening

> particular content, and families placing the computer in the living room is another example of a social technique of censorship.

Filtering can also be applied by blocking or limiting peer-to-peer (P2P) or Skype communication (Bailey & Labovitz 2011). IP address filtering and domain name system poisoning based on government-compiled blacklists of servers that should be blocked (Murdoch & Anderson 2008), and routers and government-run Web proxies to filter individual pages based on lists of forbidden keywords such as 'Falun' in the case of China (Clayton, Murdoch & Watson 2006) is also noted. In China, search engines (under pressure) have been reported to filter search results that contain certain keywords such as 'free Tibet' (OpenNet Initiative 2004). A growing number of countries are imposing mandatory requirements on Internet service providers to prevent their subscribers from accessing overseas content that would be banned under local laws. This applies to undemocratic states such as China, but also some democracies with constitutional guarantees of freedom of expression. Some countries have also put pressure on Web publishers to remove content hosted outside their jurisdiction (Anderson 2007).

Filtering is the focal point of a significant number of studies (e.g. Deibert 2003; Zittrain & Edelman 2003a, b; Hersberger 2004; Heins, Cho & Feldman 2006). There are, however also studies focusing on non-technical means of censorship, such as the use of force and intimidation through threats, beatings, prosecutions, offline surveillance and similar policies that target online journalists, bloggers and cyber activists. As an overall conclusion from such studies it seems that such acts contribute greatly to increasing levels of self-censorship (Al-Saqaf 2010).

According to Deibert and Villeneuve (2005), Internet censorship in different countries varies in terms of the types of content blocked. Repressive states block political debate (such as discussion of Tibet or the crushing of the Tiananmen Square protests in China); theocracies impose strict limits on 'blasphemous' and 'immoral' content, including information on women's rights and gay and lesbian issues (such as in Saudi Arabia and Iran); while many European states have targeted pornography and racist and xenophobic material. These countries rely on blocking technologies such as IP address-based packet filtering, domain name system poisoning, cache filtering and keyword searches (Zittrain & Edelman 2003a, b).

Another simple form of censorship is done by either charging exorbitant fees for accessing the Internet or by confining access to selected populations such as universities. While censorship has always been part of history, the Internet as a truly mass medium is more threatening to governments' control over information than earlier media (Cohen 1997), and therefore their reaction and control is much stronger where they deem it necessary or where it suites their purposes.

Data mining as a means to reflect current trends

In addition to the reports in the published and scholarly literature, the scope of Internet censorship can also be seen from mining the Internet. In this regard a number of countries were selected as representative of the global situation, namely: Australia, Chile, China, Finland, Libya, Myanmar, Singapore, Turkey, and the United Kingdom. The data mining (although it can be read against the preceding literature reviews) however, provides only partial insight into the *status quo* and intricacies of Internet censorship in each country with special reference to the selected trends and is intended as exemplars only. The data mining was conducted between January and May 2012. The process of data mining and resources used are reported elsewhere.

The amount of information available for countries differs greatly. While limited information could be traced for Chile (perhaps because we could only consider information in English) much more information was available on two democratic countries, Australia and the United Kingdom. Although there is no concern in these countries for harsh enforcement of legislation and violations of human rights, there seems to be substantial reports (because there is more freedom of speech in these countries) on concerns about trends in censorship and concerns about surveillance and breach of individual privacy. Although countries such as Australia, Finland, Turkey and Singapore motivate censorship on moral values and especially concerns about pornography and child pornography, there is evidence that other types of content such as gaming, gay practices and homosexuality is also affected by the censorship scope. Sometimes this might be evident to the population of the country (e.g. as captured in legislation or statements from government), and sometimes not. In Finland the blacklist of blocked websites is kept secret; even though incidents have been noted of websites which should strictly speaking not be blocked. In the United Kingdom the blacklist is open and available through institutions such as the Internet Watch Foundation. With regard to such blacklists there are also differences in how the list is compiled e.g. by a government body, a combination of government bodies and/or input from the general public. Some countries such as Australia and the United Kingdom rely on input from a number of sources. Reasons for the inclusion of websites on the blacklist are not always clear and in some countries such as Finland it seems as if the body or bodies compiling the list is not held responsible for the choices of websites to be blocked, or decisions on censorship seem to fall subject to arbitrary judgment by a judge. The terminology used to indicate websites to be blocked is often also vague and not clearly defined e.g. 'inappropriate', 'offensive and illegal', 'prohibited material'. This is insufficient to guide censorship.

Regardless of style of governance, dominant religion and ideology, all countries on which data were mined seem to make every effort to protect national security and stability in the country. Although, some democratic countries take strong stances on intellectual freedom, human rights, etc., it seems that concern for terrorism attacks and stability is used as a motivation for stepping up surveillance of Internet traffic and communication by all means: email, chat sessions, visits to websites, etc. This was especially evident in the United Kingdom. Although some countries like the United Kingdom expressed the need to protect personal privacy in surveillance efforts (e.g. by not monitoring communication regarding romantic relationships), such concerns, in general, do not feature strongly in their attempts at Internet surveillance. Apart from concern about the use of fear and harsh punishment to limit people's use of the Internet, most concern noted was about the surveillance and monitoring of Internet traffic and increased measures in this regard. Severe measures have been in place in countries like China, and Myanmar for some time, but it seems to be a growing concern as well in countries suspecting terrorism attacks such as the United Kingdom.

It seems as if the increase in ubiquitous means to access the Internet, also brought along an increase in the impact of the Internet on sharing and disseminating information, as well as the need to consider stricter means of control and surveillance. Concerns in this regard are strengthened by developments in countries such as Libya and Egypt where social media such as Twitter and Facebook played a major role in enforcing a change of government (Dick, Oyieke and Bothma 2012). Turkey is also noted for the growth in mobile access.

Countries are influenced by each other's policies and situations (e.g. incidents in Norway, leading to concerns and actions in the United Kingdom or Finland), country groupings (e.g. as part of the European Union), and the necessity to monitor trends and actions in other countries (e.g. the role that social media played in the unrests in Libya).

Some countries focus strongly on political reasons for Internet censorship e.g. Myanmar and China, with harsh actions against those who are in breach of legislation. Others, such as Libya claim to and (on surface level) seem to be slackening Internet censorship and the severity of actions against offenders; at the same time concerns are expressed that government control might be increasing – at least in Myanmar. An in-depth study would be necessary to confirm these perceptions. Considering the scope of Internet censorship in terms of content and scope of communication media monitored, as well as implied censorship due to very limited Internet infrastructures and search skills, more lenient government measures might easily have a very limited effect on positioning the population of the country to benefit from the advantages of the Internet.

The following table offers a brief reflection on the main impressions on each country. More detail can be found in Bitso, Fourie and Bothma (2012).

Country	**Main impressions on Internet censorship**
Australia	There are very strict regulations and measures against pornography in Australia – to such an extent that censorship in Australia has been compared with politically focused censorship in China. Many types of content other than pornography are affected by censorship such as gaming websites. The focus is, however, not explicitly politically oriented. Discrepancies between criteria for online and other media have been noted, with stricter guidelines applying to online access. Voluntary involvement of Internet service providers as well as the use of a wide variety of personal computer based filtering features in Australian Internet censorship. Although legal action and enforcement against violation of Internet censorship are reported, it is not on a level that has been considered as a violation of human rights as in other countries such as China and Myanmar. Various legislation supporting censorship, especially protection against pornography and child pornography, is in place but these seem to differ between states. In-spite of the strict regulations there seems to be some public support for even more strict control of access to pornographic information. Although it might not have a real impact on government's decisions and handling of Internet censorship, there is room for people to express themselves against Internet censorship. Electronic Frontiers Australia and the Forum on Internet Censorship, amongst others play an important role in this regard. Government websites have been targeted by cyber-attacks.
Chile	Rather limited reports (in English) could be traced on Internet censorship in Chile. Some issues that stood out are the fact that it does not seem as if Internet censorship is strongly regulated and enforced. Decisions on censorship often rely on the arbitrary views of a judge, and equipment such as hard drives have been noted to be destroyed in cases where people were held in police custody. Chile is noted for its network neutrality, and

	also attempts to make it less cumbersome for people to request public information via the Internet. It has been noted for fast speed Internet access in comparison to other countries in the region.
China	China is noted for severe measures of censorship and surveillance, as well as a lack of freedom of speech. Email and other forms of Internet communication are strictly monitored: it seems impossible to send anonymous email messages, and government security has been noted to infiltrate online systems for purposes of surveillance. Filtering software is used, and a wide spectrum of information resources are subject to censorship, e.g. websites, blogs, chat sessions, Internet telephony calls. China is not only noted for a very sophisticated system of censorship and surveillance, but also that it might have research limitations in terms of counteracting circumvention methods. More reports on side-stepping and countering censorship have been noted for China than for any of the other countries included in this study. This includes the use of circumvention software, the use of overseas ftp sites, misspelling keywords, using allegories, using web proxy servers and cryptic codes. Harsh measures are used for censorship including Internet blackouts and Denial of Service attacks, prison sentences and intimidation of journalists, bloggers and Internet content creators.
Finland	As a democratic country, reports on Finland mostly reflect concerns about pornography and specifically child pornography, as well as the protection of rights: intellectual property and copyright. It seems to be affected by terrorism incidents in other countries such as Norway to increase measures on surveillance. Concerns have been noted that Finland's censorship, in reality, covers more than pornography, and that even websites criticising censorship have been blocked. Blocking and filtering is voluntary. There are perceptions that it is easy to side-step censorship in Finland. It seems as if Electronic Frontier Finland is acting as a voice against censorship, or at least monitoring what is actually subjected to censorship. The blacklist of blocked sites is kept secret. Concern has been expressed that nobody seems to take responsibility for the choices of websites to be blocked.
Libya	Libya is marked by controversial opinions on the scope and severity of Internet censorship. Although it is no longer on the list of countries under surveillance for the list of "Enemies of the Internet", serious concerns are noted in reports, especially while Libya was under the Gaddafi rule. Although there is no formal legislation on censorship in Libya, it is marked by strong surveillance of a variety of media ranging from email to Yahoo Chat and Skype. Very few reports were picked up on concerns about the violation of personal privacy. Under the Gaddafi government, censorship was mostly politically orientated with numerous reports on actions against conduct considered as criminal. Libya is especially noted for a lack of freedom of speech. There is strong enforced reliance on cyber cafés to cooperate in surveillance. Means of censorship include blocking, curfews, blackouts and the hacking of websites.
Myanmar	Internet censorship and surveillance in Myanmar is strongly associated with violations of human rights. Although there are claims by the new

	government that they are slackening government control, opinions are voiced that government control is actually tightening. Apart from blocking websites with content in contrast to government views, and especially those of a political nature and dealing with human rights, there is severe surveillance of Internet traffic and communication, and also limits on freedom of speech. A variety of media is monitored ranging from websites and emails to Internet telephony Services. With regard to violations of privacy there is much more reported than for other countries. Myanmar is also associated with pervasive censorship – lack of Internet infrastructure for the general public and high cost for using the Internet. Apart from legislation on censorship there is also legislation on methods for circumvention of Internet censorship. Myanmar also developed means to deny the general population access to Internet content, while government officials maintain access.
Singapore	Although Singapore is not considered an "Enemy of the Internet" there is strong evidence of Internet censorship and restrictions on freedom of speech. The motivation for censorship is based on moral grounds and especially protection against pornography; thus Singapore works from a "symbolic list of 100 websites". Furthermore the claim is that the government gives preference to educate and prepare the general population to act responsibly. Although the proclaimed intention is to prevent ethnic and religious strife, it seems as if criticism against the government is also censored. There is limited reliance on technology, and sometimes the blocking of websites relies on trial and error research by Internet users to identify websites to be blocked. Different guidelines apply when deciding on websites to be blocked; these are influenced by where websites originated from (e.g. from home versus an institution) and who is accessing the information (i.e. younger or older people). Universities have been reported to maintain different Internet servers for staff and students.
Turkey	Although there is an increase in mobile access, parts of Turkey are still marked by limited Internet infrastructure and thus subject to pervasive censorship. Censorship in Turkey is aligned to the protection of families especially with regard to protection against pornography. As in many other countries, the actual scope of censorship, however, seems wider e.g. blocking websites with negative information on Mustafa Kemal Atatürk (considered as the father of modern Turkey by many). Concerns on violation of individual privacy did not quite feature in the data mined. Turkey uses a centralized system of filtering, and there is a lack of transparency in terms of websites blocked. Although there initially was no formal legislation on censorship and surveillance, there are moves in this direction. Faced by large scale national protests against Internet filtering, steps were taken to prevent attacks on government websites. There also seems to be a rise in government censorship with actions being taken against websites supporting actions against censorship. Earlier in 2012 large numbers of people participated in national protests against Internet filtering. Positive trends in Turkey include the fact that the content of

	blocked websites can sometimes still be accessed, as well as the support the Alternative Informatics Association offers for Internet users opposing censorship.
United Kingdom	Although a democratic country, the United Kingdom seems to have very strict rules on Internet censorship and especially Internet surveillance, owing to a strong concern for national security. Deep-packet inspection technology is used and surveillance includes the use of mobiles and YouTube. Although incidents of legal actions have been reported, these do not seem extreme when compared to countries like China or Myanmar. Recently the United Kingdom has experienced a number of cyber-attacks by groups against Internet censorship and surveillance. Although initially there was no legislation – only with regard to issues such as pornography and the protection of children, the United Kingdom have accepted legislation and is considering even further legislation on various issues related to Internet censorship and surveillance owing to national security, data protection and privacy. Current legislation gives strong control to representatives of the government – a concern for those against censorship. Much criticism against the government's actions and plans were noted in the mined data, which points to stronger freedom of speech than in other countries monitored.

Trends in Internet censorship based on Internet data mining

With regard to the trends monitored, information was mostly found on the negative trends of the filtering and blocking of Internet content, and especially increased surveillance of all media related to Internet access including mobiles and voice telephony calls. Detailed discussions of the trends are available at http://www.ifla.org/en/node/6713. Table 2 which follows offers a brief reflection on the main impressions per trend. All countries are influenced by what happens in other countries e.g. terrorism attacks such as in Norway or uprisings in Egypt and Libya, and the overthrow of governments in the latter. Some countries are also marked by increased restrictions on the freedom of speech.

Table 2: Trends in Internet censorship

Country	Main impressions on Internet censorship
Negative trends	
Internet related privacy	In many countries strong trends toward nation-wide monitoring, sometimes even calling on the support of search engines such as Google, Internet café owners and Internet service providers, were noted. In some countries serious invasion of individual privacy are noted e.g. people not being able to send anonymous emails, and government security infiltrating online networks. In some contexts

	the rationale is for preventing criticism against the government and in others for national security. In some countries strong surveillance was noted, but limited reports on reactions to invasion of privacy were picked up through data mining.
Ubiquitous society and control	Various bodies are involved in control, ranging from governments and bodies of authority mandated by them, to a strong reliance on Internet service providers, and also Internet café owners (even by enforcement). Sometimes this is supplemented by the use of filtering software on personal computers and calls on parents to accept more responsibility. Especially in Myanmar strong reliance on Internet café owners were noted.
Internet related media being censored	Although mostly websites are targeted, censoring of social media websites, chat groups, and Internet telephony service (e.g. Skype) also occur. In some countries Internet censorship is formerly regulated by the government; in others there are no formal legal structures but very strong surveillance and enforcement actions.
Filtering and blocking Internet content & blocking software	Blacklists of websites to be blocked depend on input from various resources: body of authority assigned by the government, combination of bodies of authority, input from blacklists compiled by other countries, trial and error research and input by the public. The United Kingdom uses, amongst others, trained police analysts. Some blacklists are available, while others are kept secret – even in democratic countries such as Finland. Some countries, such as Singapore proclaim a "symbolic list of 100 websites". From the spectrum of content addressed by censorship, political issues and anti-government sentiments and actions, and pornography stand out. There is, however, evidence that it often stretches much wider than the proclaimed foci of e.g. pornography and moral values to include criticism against political leaders, calls for human rights, and criticism of censorship. The sophistication of Internet filtering differs widely across countries e.g. ranging from layered filtering to specialist software such as Websense and Cleanfeed to filtering software for personal computers. Filtering ranges from voluntary to mandatory and legally enforced. In some countries filtering is also aimed at protection of intellectual copyrights. Some countries e.g. Singapore claim to rather focus on educating and preparing the general population to react responsibly. Different guidelines on levels of blocking depend on origin of generation and who is accessing the information. Censorship is also aimed at the protection of families, and political leaders such as in Turkey.
Monitoring technologies	Although not much was picked up by data mining, the use of specific software was noted. Sometimes, as in the case of Libya and Myanmar, such software is even provided with help from companies in democratic countries. Cross country expertise is also employed in censorship e.g. drawing on experts from Russia, Pakistan and Poland (in the case of Libya). A wide variety of software is used.

	Some countries rely strongly on technology while others are marked by limited reliance and even trial and error research by Internet users (e.g. Singapore). The United Kingdom uses deep-packet inspection technology. Many countries are planning to step up on surveillance technology.
Criminalization of legitimate expression on the Internet	Actions against those considered in breach of regulations and legislation differs widely between countries. It can range from a fine, police custody, imprisonment, intimidation and even alleged murder. Actions in some countries such as China and Myanmar are so severe that it is actually seen as violations of human rights.
Acts, regulations and legislation	The scope of legislation in countries differs widely. Some countries have various supporting legislation ranging from child protection and legislation against pornography to legislation dedicated to Internet censorship and surveillance of communication. Chile was noted for its legislation on network neutrality. In Myanmar there is even banning of Internet censorship circumvention.
New forms of Internet censorship	Very little was noted on new forms of censorship. Data mining focusing specifically on forms noted in the subject literature such as Halaal censorship might be more effective. Methods that were noted include curfews, blackouts, and denial of service attacks. Although not new, pervasive methods, such as poor Internet infrastructures and high cost of Internet use, should get more attention.
Support for Internet censorship	Although very diverse opinions on censorship are noted, and although opinions expressed via Internet communication channels are often against Internet censorship and especially surveillance, there are from time to time calls for stricter censorship coming from the public.
Enforcing regulations and Internet censorship	Great diversity was noted between countries, ranging from rather lenient e.g. fines and blocking websites to harsh prison sentences and the use of fear and punishment to put pressure on people to keep to regulations.
Internet related communication surveillance	In democratic countries especially, such as the United Kingdom a strong trend towards nation-wide surveillance was noted. Very heavy surveillance in China, Myanmar (seeming to draw on all possible resources) and Libya were noted. The United Kingdom, Finland and Turkey are also considering stricter surveillance.
Positive trends	
Reactions to Internet censorship	Cyber-attacks on key websites such as those of the government, activities of anti-censorship groups and even large scale protests such as in Turkey are used to relay the feeling of the public or specific interest groups. Dedicated groups such as Electronic Frontier Australia, Reporters Without Borders and the OpenNet Initiative also make considerable contributions in raising awareness of the scope and form of Internet censorship. Where censorship is politically focused, some countries claim to be slackening control with a change of government such as in Myanmar and Libya. There

	are, however, some doubts about this.
Attempts and means to side-step Internet censorship	The use of circumvention software, overseas ftp sites, misspelling of keywords, allegories, web proxy software, and cryptic codes were noted.
Cyber actions against Internet censorship	Some incidents of cyber-attacks on key websites such as those of the government are increasing as a means to express anti-censorship sentiments.
Innovative ways of showing opposition to Internet censorship	Relatively little was noted on innovative ways of showing opposition to Internet censorship. Data mining focusing specifically on means of showing opposition as noted in the subject literature might be more effective. Search engines such as Google have voiced concerns about the plans of some countries, and some politicians have been noted to speak out against Internet censorship. Support from specialists such as Global Internet Freedom, and the Global Internet Freedom Fund strengthens the case of those against censorship. Often criticism from outside a country is noted as well as from international monitoring services such as OpenNet Initiative and Reporters Without Borders.

Conclusion

Censorship or protection, intellectual freedom or provision of an environment where children are safe from exploitation represents a big debate (Clyde 1997). The important issue is to understand what censorship is, as well as its norms and to appreciate that it has been practiced for years and is inherent to society, even more so in electronic environments, hence the existence of Internet censorship. The societal issues such as concerns about the use of the Internet and how they can be addressed through censorship, the rationale for censorship including parties responsible for it as well as arguments supporting or refuting censorship are all important even though they are not simple to address. It is equally important to constantly follow trends on Internet censorship including tools and techniques that are used as well as means of countering them. Censorship in various contexts is deeply rooted in people's professional ethics, beliefs concerning intellectual freedom, lifestyle choices, religious beliefs, attitudes to children and ideas about the rights of other people in a democratic society (Clyde 1997).

The article started by stating the benefits of the Internet as providing access to all people on all levels of society to access all kinds of information. Actions such as filtering, blocking and legal action against people affects the informedness of people, their ability for decision-making, educational opportunities and insights in e.g. other religions and ideologies. With Internet censorship such opportunities for people to be empowered are affected and denied with regard to various facets of everyday life: politics, religion, health, education, social interaction, etc. Apart from education, the effect of Internet censorship on other advantages of the Internet does not seem to be seriously addressed in the scholarly literature. There is a need for research to assess the impact of Internet censorship on various facets of information practices and information behaviour. Furthermore, research on Internet censorship and the ethos of information ethics is also crucial.

References

Akdeniz, Y. 2007. Governing racist content on the internet: national and international responses. *University of New Brunswick law journal* 56: 103-161.

Akdeniz, Y. 2008. *Internet child pornography and the law: national and international responses.* London: Ashgate.

Akdeniz, Y. and Altiparmak, K. 2008. Internet: restricted access: a critical assessment of internet content regulation and censorsip in Turkey. http://privacy.cyber-rights.org.tr/?page_id=256. Accessed 3 March 2012.

Al-Saqaf, W. 2010. Internet censorship challenged - how circumvention technologies can effectively outwit governments' attempts to filter content. Alkasir case study. In Strand, C. *Increasing transparency and fighting corruption through ICT: empowering people and communities.* Stockholm: SPIDER - The Swedish Program for ICT in Developing Regions, pp. 71-89.

Anderson, M. 2007. Internet censorship: as bad as you thought it was - maybe a bit worse, actually. http://spectrum.ieee.org/telecom/internet/internet-censorship-as-bad-as-you-thought-it-was. Accessed 26 March 2012.

Ang, P. and Nadarajan, B. 1996. Censorship and the internet: a Singapore perspective. *Communications of the association for computing* 39(6): 72-78.

Bailey, M. and Labovitz, C. 2011. Censorship and co-option of the internet infrastructure. Technical report, CSE-TR-572-11. http://nsrg.eecs.umich.edu/publications/CSE-TR-572-11.pdf. Accessed 6 March 2012.

Bambauer, D. E. 2009a. Cybersieves. *Duke law journal* 59(3): 377-446.

Bambauer, D.E. 2009b. Filtering in Oz: Australia's foray into internet censorship. *University of Pennsylvania journal of international law* 31(2): 493-530.

Bernstein, M. 2004. Internet censorship in the hospital: bad ethics and great irony. *Healthcare quarterly* 7(4): 8-9.

Bihani, S. and Hamilton, S. 2009. Third meeting of the internet governance forum (IGF), Hyderabad, India. *IFLA journal* 35(1): 59-62.

Bitso, C., Fourie, I. and Bothma, T. 2012. Trends in transition from classical censorship to Internet censorship: selected country overviews (contract research for a FAIFE, IFLA project commissioned by Prof Kai Ekholm, National Librarian, Finland published as a FAIFE Spotlight). http://www.ifla.org/publications/trends-in-transition-from-classical-censorship-to-intenet-censorship-selected-country-o. Accessed 31 July 2013.

Calingaert, D. 2010. Authoritarianism vs internet. *Policy review* 160: 63-75.

Clayton, R., Murdoch, J. and Watson, N.M. 2006. Ignoring the great firewall of China. *I/S: A journal of law and policy* 3(2): 271-296.

Clyde, A. 1997. Censorship or protection? Children and acess to the internet. *Emergency librarian* 24(3): 48-50.

Cohen, T. 1997. *Censorship and the regulation of speech on the internet*. Johannesburg : Centre for Applied Legal Studies.

Colaric, S. 2003. Children, public libraries, and the internet: is it censorship or good service? *North Carolina Libraries* 61(1): 6-12.

Dahan, I., Raitt, D. and Jeapes, B. 1995. The internet and government censorship: the case of the Israeli secret. In proceedings of the International Online information meeting no.19, London, 5-7 December 1995. http://cat.inist.fr/?aModele=afficheN&cpsidt=3151446. Accessed 20 March 2012.

Deibert, R. 2003. Black code: censorship, surveillance and the militarisation of cyberspace. *Millennium - journal of international studies* 32(3): 501-530.

Deibert, R. and Villeneuve, N. 2005. Firewalls and power: an overview of global state censorship of the internet. In Klang, M. and Murray, A. eds. *Human rights in the digital age*. Portland, Or.: GlassHouse.

Deibert, J.G., Palfrey, R., Rohozinski, R. and Zittrain, J. eds. 2008. *Access denied: the practice and policy of global internet filtering*. Cambridge, MA: MIT Press.

Deibert, J.G., Palfrey, R., Rohozinski, R. and Zittrain, J. eds. 2010. *Access controlled: the shaping of power, rights, and rule in cyberspace*. Cambridge, MA: MIT Press.

Deibert, J. G., Palfrey, R., Rohozinski, R. and Zittrain J. eds. 2012. *Access contested: security, identity, and resistance in Asian cyberspace*. Cambridge, MA: MIT Press.

Deibert, R. and Rohozinski, R. 2010. Liberation vs control: the future of cyberspace, *Journal of democracy* 24(1): 43-57.

Depken II, C. A. 2006. Who supports internet censorship? *First Monday*, 11(4). http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1390/1308. Accessed 12 February 2012.

Dick, A.L., Oyieko, L.I. and Bothma, T.J.D. 2012**.** Are established democracies less vulnerable to internet censorship than authoritarian regimes? The social media test. http://www.ifla.org/publications/are-established-democracies-less-vulnerable-to-internet-censorship-than-authoritarian-r. Accessed 31 July 2013.

Dickinson, D. 1997. The internet in China: embarking on the "information superhighway" with one hand on the wheel and the other hand on the plug. *Journal of international law,* 1996 -1997 15(3): 621-642.

Duke, A. C. and Tamse, C. A. eds. 1987. *Too mighty to be free: censorship and the press in Britain and the Netherlands.* Zutphen: De Walburg Press.

Editors of the Public Library Quarterly. 2008. Learning sites, references and notes. *Public library quarterly* 27(3): 274-289.

Electronic Frontiers Australia. 2002. Internet censorship: law and policy around the world. https://www.efa.org.au/Issues/Censor/cens3.html. Accessed 26 January 2012.

Faris, R. and Villeneuve, N. 2008. Measuring global internet filtering. In Deibert, J.G. *et al*. eds. *Access denied: the practice and policy of global internet filtering*. Cambridge, MA: MIT Press, pp. 5-27.

Feamster, N. et al. 2002. Infranet: circumventing web censorship and surveillance. In Proceedings of the 11th USENIX conference on security. USENIX Association; USENIX Security'02, pp. 247-262. http://static.usenix.org/event/sec02/feamster/feamster_html/. Accessed 3 March 2012.

Frechette, J. 2005. Cyber-democracy or cyber-hegemony: exploring the political and economic structures of the internet as an alternative source of information. *Library trends* 53(4): 555-575.

Gorman, G. 2005. China-bashing in the internet censorship wars. *Online information review* 29(5): 453-456.

Grothoff, *et al*. C. 2003. *An encoding for censorship-resistant sharing*. Technical report. http://www.cs.helsinki.fi/u/jtlindgr/stuff/ecrs.ps. Accessed 6 February 2012.

Hadfield, A. ed. 2001. *Literature and censorship in renaissance.* Hampshire: Palgrave.

Heins, M., Choc, C., and Feldman, A. 2006. *Internet filters: a public policy report*. 2nd ed. New York: New York University School of Law.

Hersberger, J. A. 2004. Internet censorship. In Bidgoli, H. ed. *The internet encyclopedia*, 2. Hoboken, NJ: John Wiley and Sons.

IFLA. 2012. IFLA calls on the Chinese government to end censorship of internet access and allow freedom of expression online. http://www.peacehall.com/news/gb/english/2005/07/200507150101.shtml. Accessed 20 March 2012.

Johnson, D. 1998. Internet filters: censorship by any other name? *Emergency librarian* 25(5): 11-13.

Karhula, P. 2011. Freedom to read? – Getting a picture of internet censorship. Signum. http://www.ojs.tsv.fi/index.php/signum/article/download/4397/4107. Accessed 4 February 2012.

Malley, I. 1990. *Censorship and libraries.* London: Library Association Publishing.

McDonald, F.B. 1993. *Censorship and intellectual freedom: a survey of school librarians' attitudes and moral reasoning.* London: Scarecrow Press.

Munro, C.R. 1979. *Television, censorship and the law*. Aldershot: Gower Publishing Company.

Murdoch, S.J. and Anderson, R. 2008. Tools and technology of internet filtering. In Deibert, J. *et al*. eds. *Access denied: the practice and policy of global internet filtering*. Cambridge. MA: MIT Press, pp. 57-72.

Oboler, E. M. 1980. *Defending intellectual freedom: the library and the censor.* Westport: Greenwood Press.

OpenNet Initiative. 2004. Probing Chinese search engine filtering. http://opennet.net/bulletins/005/. Accessed 25 January 2012.

Peace, A. 2003. Balancing free speech and censorship: academia's reponse to the internet. *Communications of the Association for Computing Machinery* 46(11): 105-109.

Robotham, J. and Shields, G. 1982. *Freedom of access to library materials.* New York: Neal-Schuman Publishers.

Thompson, A. H. 1975. *Censorship in public libraries in the United Kingdom during the twentieth century.* Essex: Bowker.

Truett, C. 1997. Censorship and the internet. *School library media quarterly* 25(4): 223-227.
Wang, C. 2003. Internet censorship in the United States: stumbling blocks to the information age. *IFLA journal* 29(3): 213-221.

Warf, B. 2011. Geographies of global internet censorship. *Geojournal* 76(1): 1-23.

Wikipedia. http://www.wikipedia.org; Accessed 16 February 2012

Zittrain, J. and Edelman, B. 2003a. Internet filtering in China. *IEEE Internet Computing*, March/April, 69-77.

Zittrain, J. and Edelman, B. 2003b. *Internet filtering in China.* Harvard Law School. Research paper no. 62. http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan011043.pdf Accessed 16 February 2012.

Zittrain, J. and Palfrey, J. 2008a. Introduction. In: Deibert, J. G. *et al*. eds. *Access denied: the practice and policy of global internet filtering*. Cambridge, MA: MIT Press, pp. 1-4.

Zittrain, J. and Palfrey, J. 2008b. Internet filtering: the politics and mechanisms of control. In: Deibert, J. G. *et al*. eds. *Access denied: the practice and policy of global internet filtering*. Cambridge, MA: MIT Press, pp. 26-56.