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

Dr Constance Bitso
Department of Information Science, University of Pretoria, Lynnwood Road, Pretoria, South Africa, 0002. Email: connie.bitso@up.ac.za

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

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

CONTENT

Abstract: Censorship is no longer limited to printed media and videos. Its impact is felt much more strongly with regard to 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), as well as initiatives to counter censorship. The article reflects on trends in Internet censorship in selected countries, namely Australia, Chile, China, Finland, Lybia, Myanmar, Singapore, Turkey, and the United Kingdom (UK). These trends are discussed under two broad categories of negative and positive trends. Negative trends include: trends in 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. Detailed reports for each country are included as appendixes. A summary of how the trends manifest in the countries in which data were mined, as well as the trends *per se* is included in the article.

Keywords: Internet censorship, e-censorship, trends, Australia, Chile, China, Finland, Lybia, Myanmar, Singapore, Turkey, United Kingdom (UK)

1 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). Munro (1979:4), explains that censorship is a convenient description encompassing all the processes whereby the dissemination of information, opinions or ideas are suppressed. According to Malley (1990:2), censorship is polarised along political lines such that political control determines what may or may not be censored; and thus involves the banning of material on political grounds. Censorship is totally different from 'selection' which matches information sources with users' information needs and it is usually exercised in accordance with the law of the country in which it is being practiced (Malley, 1990:29).

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 the trends in the transition from classical censorship to Internet censorship, this article briefly reflects on the background to traditional censorship, the clarification of key concepts, brief reference to the literature on Internet censorship, the identification of trends to monitor, and the tools that were used for data mining.

2 BACKGROUND ON TRADITIONAL CENSORSHIP

Censorship is a long-lasting operation (Oboler, 1980:80), and as such it has been part of human history. There is no evidence that it is likely to decrease (Robotham & Shields, 1982:58); in fact it seems to be increasing in some countries. It 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 & Shields, 1982:58). There are various reasons for censorship; sometimes information is censored because of political, social, economic, religious, philosophical, moral, ideological, military, corporate, and educational reasons, where people feel material offers an attack on themselves and their personal values (Oboler, 1980). The focus and the degree of such censorship differ between countries.

Censorship is evident in various contexts such as public libraries (Thompson, 1975), school libraries (Oboler, 1980), and in press as evidenced in the monograph on censorship and the press in Britain and the Netherlands edited by Duke and Tamse (1987). Such censorship often takes the form of e.g. age restriction and parental guidance. It is also evident in other contexts such as theatre, religion and politics as revealed in a monograph edited by Hadfield (2001) on literature and censorship in England. In that monograph there is also evidence that censorship was applied to educational sources, music and entertainment, pictures, etc. Therefore, censorship can take many forms. For instance, McDonald (1993:5) alludes to voluntary censorship which occurs when the librarian, as a result of real or anticipated pressures from school boards and communities, removes or restricts resources or does not purchase certain titles.

3 CLARIFICATION OF TERMINOLOGY

With the introduction of the Internet different forms of censorship and different motivations for censorship have evolved. Terminology that is used includes e-censorship, cyber censorship, Net censorship and Internet censorship. For purposes of this article the concept “Internet censorship” will be used. Wikipedia distinguishes different types of censorship: meta-censorship, Internet censorship, and creative censorship. According to Wikipedia (http://en.wikipedia.org/wiki/Internet_censorship), Internet censorship concerns the control or suppression of the publishing and accessing of information on the Internet carried out at different levels such as governments, private organisations and individuals.

3.1 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” (http://en.wikipedia.org/wiki/Internet_censorship).

3.2 Meta-censorship

In this form of censorship, any information about existence of censorship and the legal basis of the censorship is censored, rules of censoring are classified, and removed texts or phrases are not marked (http://en.wikipedia.org/wiki/Internet_censorship).

3.3 Internet censorship

Unlike censorship in other areas, Internet censorship is a relatively new phenomenon and remains seriously under-researched. Censored content varies widely based on country, culture and context, and may range from child pornography to gambling as well as censorship of dissident content (Al-Saqaf, 2010).

4 BACKGROUND ON INTERNET CENSORSHIP

As early as the 1990’s when proliferation of the Internet started, countries were already enacting legislation on Internet censorship. This is evidenced by Cohen (1997:12) who noted that at the time more than 30 countries have enacted or are in the process of enacting Internet specific censorship legislation. The rationale advanced for these censorship measures include routine motivations such as the desire to protect children, public morals, public safety, political objectives, and to silence racists and hate speech. Despite disparities in policy, types of governance and divergent approaches in adherence to international human rights treaties, restrictions on Internet access and content were noted to be increasing worldwide in 1997 (Cohen, 1997); it is now even more so. Along with the rapid growth in Internet use, Internet censorship has also become increasingly visible; it has started to gain attention from scholars and research institutions in different disciplines including media and communication, information technology, law, political science, and economics. Reports dealing with Internet censorship have also been 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 a rather complex subject as it is comprised of several aspects that have to do with the Internet's structure and application as well as Internet users' behaviour, and state control, along with several other factors that vary based on the socio-economic and political situations of the country in question (Al-Saqaf, 2010).

A study of Internet censorship need to consider the concerns for censorship which must be weighed against the abundance of opportunities and benefits that came with the introduction of the Internet, as well as the concerns for the un-censored use of the Internet.

5 BRIEF REVIEW OF FORMAL, SCHOLARLY REPORTS ON INTERNET CENSORSHIP

This section briefly reviews articles, dissertations, books, conference papers, and web policy documents to capture the essence reported on issues of Internet censorship. Databases searched include ISI Web of Science, Library and Information Science Abstracts (LISA), Library and Information Technology Abstracts (LISTA), ScienceDirect and Emerald. Formal, scholarly literature is marked by arguments, concerns, and steps taken regarding Internet censorship. A preliminary review already revealed that 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, and also that a limited number of countries is covered.

Censorship can be enforced by many stakeholders such as universities, schools, parents, and individuals' self-censorship. The government is the most important enforcer of censorship as will be reflected in the country reports. The state can also block Web pages, websites and other Internet information resources. Various means of filtering by the State can be noted (e.g. as discussed in *Access Contested: Security, Identity; and Resistance in Asian Cyberspace* (Deibert *et al*., 2012), *Access Controlled: the Shaping of Power, Rights, and Rule in Cyberspace* (Deibert *et al*., 2010) and *Access Denied: the Practice and Policy of Global Internet Filtering* (Deibert *et al*., 2008). Faris and Villeneuve (2008:7) offer a list of various categories of information subject to Internet filtering. These include the more obvious such as political transformation and information by opposition parties, political reform, legal reform and government, 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.

5.1 Internet advantages and opportunities affected by censorship

The Internet is a social, cultural, commercial, educational, and entertainment global communications system whose legitimate purpose is to benefit and empower online users, also lowering the barriers for the creation and the distribution of content throughout the world. Although it resembles traditional methods of communication, it differs from many given that it is the largest global communication network and completely decentralized with invisible boundaries (Akdeniz & Altiparmak, 2008). As such it was concluded that nobody owns the Internet, and there is no single entity, nor single government governing the Internet (Cohen, 1997). It is universally accepted that information and communication technologies can significantly enhance the exercise 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, while they may badly affect these rights, freedoms and values, such as the disrespect for private life and secrecy of correspondence, and the dignity of human beings (Akdeniz & Altiparmak, 2008).

The Internet has brought opportunities for any person to communicate instantly with a huge international audience (Cohen, 1997). It has unleashed a wide-range and a global shift in communication that significantly empowers individuals (Deibert & Rohozinski, 2010). Ironically, since the Internet became popular and widely accessible in the mid-1990s, the availability of certain types of content defined broadly as illegal and harmful, has become the focus of many governments, regulatory agencies, and international organizations. Consequently, nations try to resolve Internet content related problems by means of introducing new laws or amending existing laws (Akdeniz & Altiparmak, 2008).

Easy and inexpensive access to the Internet, as well as the development of the World Wide Web, provided new and ready opportunities for global publishing but unfortunately this extended to material of a racist nature, as well as other undesirable material such as pornography (Akdeniz, 2007). Flyers and pamphlets that had traditionally been distributed locally by hand and had limited visibility can now be distributed and accessed globally through the Internet (Akdeniz, 2007). This is a great advantage of the Internet to reach masses of people instantly. However, alongside this is a founded prediction that the dissemination of racist content and other undesirable material would increase with the rapid growth of Internet use around the globe; this may force censorship to be implemented.

According to Cohen (1997:13), while governments recognise that the benefits of the Internet far outweigh its negative aspects, they maintain that these negative aspects cannot be ignored as they are seen as pressing issues of public, political, commercial and legal interests. As a result, some governments go beyond ensuring a safe environment for minors and traders, and limit the liberalising effect of the Internet by denying access to entire segments of their populations.

For centuries universities have been regarded as upholders of free speech and as places where censorship is undesirable because students are given the freedom to explore differing opinions. However, this attitude was developed at a time when information flowed less freely than in today's world of the Internet (Peace, 2003). Nevertheless, one does not dispute that the Internet has an advantage to offer university students and the entire academia a global platform to exchange and access information. Technology has made available a wealth of knowledge, but along with websites dedicated to scholarship and harmless entertainment are websites that 'promote pornography, racism, and criminal activity’ (Peace, 2003). The question is: should universities allow this material to be easily used on campus computer labs and residence halls? Peace (2003) notes that a conflict exists between the rights of students and the ideology of free speech and privacy, and the obligations of universities, parents, and society to restrict access to information deemed unsuitable for the youth. The communal nature of academia further complicates matters because controversial information is often accessed in computer labs, potentially exposing other computer users to information they may find offensive (Peace, 2003). In such situations, Internet censorship is seen as a solution to the situation.

According to Clyde (1997), the Internet is considered as an important educational resource; yet there is considerable evidence of the feeling that the Internet is an environment from which children must be protected. This is because there is evidence that the Internet is also a platform filled with illicit issues such as pornography and formulas for drugs or bombs, where paedophiles and rapists stalk the innocent and is marked by disorder and lawlessness (Clyde, 1997). These negative views about the Internet tend to influence what happens at the school level because even though there are useful educational programs available through the Internet, these negative vibes pose challenges to parents, teachers and school librarians about the use of the Internet by school children.

5.2 Concerns of Internet use that can be addressed by censorship

One of the major concerns of Internet use is the freedom to post information on the Web which is unlimited in some instances without a review process. It is a platform where 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, because the credibility of some websites is questionable. Although children and everyone using the Web, need to learn to analyze and challenge the authority of documents on the Web, and not just assume the document is credible (Colaric, 2003), it is still not known at all if children are able to do this and at what stage they can do it. Thus it is often argued that censorship may be useful when it comes to children.

According to Depken II (2006) concerns of Internet use that led to censorship of the Internet have focused on a wide range of topics, 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. Hence, Internet censorship movements have taken two predominant forms to limit what can be viewed or what can be posted on the Internet (Depken II, 2006).

Increasing digitisation of information led to a wide range of consumer products, including movies, music, and books to be easily distributed to consumers. Although entertainment, software, and other commercial industries have sought to capitalise on new means of distributing their products through digital networks, they have to face the problem of theft of intellectual property as well as copyright violations. There is a major concern that once information is digitised and placed on distributed networks, it is easy to duplicate and distribute (Deibert, 2003) and therefore it is deemed censorship could help in that situation.

5.3 Who is responsible for censorship?

Censorship is intertwined with social responsibility. Therefore in any country the system of social responsibility also becomes responsible for censorship (Malley, 1990:21). It is therefore not surprising to find, as indicated earlier, parents, teachers, clergy, politicians and other social groups in the limelight of some form of censorship. It is evident that censorship needs to be practiced within a legal framework in order to be implemented effectively. As a result Malley (1990) articulates on censorship and the law; and Cohen (1997) also approaches censorship and the regulation of speech on the Internet from the legal perspective. As a result, developers of legal frameworks are also stakeholders for censorship.

Censorship of various forms is also part of government systems. This is what is mostly reflected by data mining, and that applies to democratic governments such as Australia and the United Kingdom as well as authoritarian governments such as China and Myanmar. While deliberations of this article to this end have been on censorship of information, Merrett (1994) brings to light other aspects of censorship applied to people in Apartheid South Africa such as banning, deportation, torture and murder. This is a testimony of a government responsible for a policy on human censorship. It thus seems that governments may be responsible for censorship through legal frameworks, regulations and policies at various levels: national, federal, local, etc. In addition, an article by Dahan *et al*. (1995) and regional overviews and country summaries in the book *Access denied: the practice and policy of global Internet filtering* (Deibert *et al*., 2008) supports perceptions of governments being responsible for censorship. More testimonies are outlined in Appendix B with the country reports.

Other parties responsible for censorship that have been noted in the literature include Internet users in content rating systems and privatised censorship (Akdeniz, 2008); school librarians and teacher-librarians (Truett, 1997); public librarians (Colaric, 2003) and hospitals' management (Bernstein, 2004).

5.4 Categorisation of responses against and for censorship

The Internet today is standing at a threshold; both limitless opportunities and daunting threats lie ahead. The challenge is to grab the opportunities and exploit them to the fullest, while containing, if not eliminating, the threats (Bihani & Hamilton, 2009).

People in support of censorship such as Cohen (1997) argue that information over the Internet is controlled because open communication technology carries a certain amount of potentially harmful or illegal content. The fear is that it can be used as a vehicle for criminal activities and terrorism. However, those that are against the issue indicate that the primary motivation for the co-option of Internet infrastructure to effect filtering is political. Whether the filtering of content in China and Iran or the wholesale blocking of traffic in Myanmar (also known as Burma) or in Egypt, filtering as a form of censorship seeks to influence the spread of ideas and to limit communication within the global community (Bailey & Labovitz, 2011). In addition, the fight against censorship is based on the defence of intellectual freedom which has always been the essence of Information Science (Malley, 1990). Maybe the most worrying part in the new forms of censorship is that they become mostly hidden from the users (Karhula, 2011). This view is supported by some of the country reports in Appendix B.

The perceived need for information filtering is an inevitable consequence of the information explosion. Whether it is considered for good or for evil, the selection or de-selection of information is necessary, given each individual's ability to absorb and to discriminate information (Malley, 1990).

Another important argument supporting censorship is that there is general agreement on the need to intensify efforts to combat cyber-crime mainly because the growth of the Internet has created opportunities for cyber hackers and criminals (Bihani & Hamilton, 2009). Viruses, spyware, phishing and botnets are obstacles to the future growth of the Internet that cannot be ignored and as such cyber security is becoming not only important, but also more and more complex with every advance of technology (Bihani & Hamilton, 2009).

Nonetheless, an important librarian perspective from Johnson (1998) is that library training instils support of free, uncensored access to information for children, as well as for adults, regardless of format. Thus the existence of potentially objectionable materials should not be used as a reason to deny children access to the Internet. At the present time, the Internet is an all or nothing proposition for schools and libraries because controlling devices, such as filters and rating systems, either do not work, or eliminate the best features of the Internet. While these devices may be appropriate for use by parents on home computers or for use by private institutions, their use conflicts with perceptions of intellectual freedom and the mission of public institutions (Johnson, 1998).

In addition, Johnson (1998) argues that students need to be given the freedom, responsibility, and training to make good decisions instead of practicing censorship. The reason being real learning, the genuine practice of exercising one's ability to make good choices, cannot occur in a protected and censored environment that never gives one the chance to make mistakes (Johnson, 1998). He cites Howard Reingold’s argument that, "the only protection that has a chance of working is to give our sons and daughters moral grounding and some common sense".

Although motivations for Internet censorship differ from country to country, Cohen (1997) identifies a number of concerns common to many countries that lead to censorship, namely:

- National security (weapons’ making, illegal drugs and protection from terrorism)
- Protection of minors (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 (unauthorised communication of personalised data, electronic harassment, spamming)
- Protection of reputation (defamation, unlawful comparative advertising)
- Intellectual property (the unauthorised distribution of copyrighted works such as music, software, books, etc.)

Finally, the debate supporting or opposing censorship hits hard on professional groups such as teachers because they are caught right in the middle of the debate about censorship and freedom of access, as they are ultimately responsible for the safety of their pupils and students when they access the Internet, while also being charged with a duty to educate (Lawson & Comber, 2000).
As the country reports in Appendix B will show, data mining picks up mostly political and governmental inflicted censorship.

5.5 Means to counteract Internet censorship

Studies such as Al-Saqaf (2010) reveal some means to counteract Internet censorship. The intention of the study was to prove that censorship circumvention techniques are able to challenge Internet censorship of dissident content. It came at a time when censoring online content critical of governments had reached high levels, particularly in regions witnessing unprecedented growth rates in Internet use such as China, Iran and Arab countries.

In another instance, there is evidence that with little effort, users are able to evade filters by accessing blocked websites 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) (Feamster *et al*., 2002). Even countries such as China that have made a concerted effort to block user access to such proxies find it difficult to locate and filter every single proxy machine. Anticensorship activists have also developed proxies that individual users can run on their home and office personal computers (PCs) anywhere in the world, making it extremely difficult for governments to block access to every proxy (Feamster *et al*., 2002). The country reports in Appendix B reflect only a few initiatives in this regard; perhaps with good reason.

Dahan *et al*. (1995) proclaims the Internet as a tool for bypassing government censorship and internal censorship (censorship and sanctions by service providers, self-censorship and 'netiquette'). This is done through the use of anonymous remailers and encryption software tools that allow anonymous dissemination of information.

6. COUNTRIES AND INTERNET CENSORSHIP: A BRIEF REVIEW OF THE LITERATURE

From the preface of the book *Accessed controlled: the Shaping of Power, Rights, and Rule in Cyberspace* (Deibert *et al*., 2010) one gathers that 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; China's famous "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). OpenNet Initiative research ranks filtering as: pervasive filtering, substantial filtering, selective filtering, suspected filtering and no evidence of filtering. Frechette (2005) alludes to over regulation and under regulation of the Internet. Discussion in the following paragraphs is offered as background to the detailed reports in Appendix B on selected countries.

Bambaeur (2009) points out that while censorship in some countries such as China is highlighted in papers and receives much attention, censorship in other countries such as the United States of America does not feature so prominently. IFLA’s call on the Chinese Government to end censorship of the Internet is one example of such highlights (http://www.peacehall.com/news/gb/english/2005/07/200507150101.shtml).

Bambaeur (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 in various countries 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). Nonetheless, through censorship most countries try to make content disappear from the Web. Whether it's copyrighted songs in America or political dissent in Iran, the goal is the same, it is only the targeted material that varies. 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).

The books *Access Denied (*Deibert *et al*., 2008)*, Access Controlled (*Deibert *et al*., 2010) and *Access Contested (*Deibert *et al*.*,* 2012) outline a summary of selected countries based on the OpenNet Initiative research. In the books it is explained 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. Nonetheless, the books allude to 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 any other issue 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.

As pointed out earlier, the Internet is rapidly gaining worldwide popularity. As an apparently borderless technology, it has given rise to tremendous information-sharing capabilities. Although several nations have been eager to embrace the Internet, the development of the Internet has given rise to controversies over the acceptable limitations on individual speech and expression. China is a nation which has traditionally kept the dissemination of information and freedom of expression to a minimum. Therefore, there is a dilemma between the Internet's seemingly limitless potential for global communication and the Chinese government's desire to control the flow of information in and out of the country (Dickinson, 1997). Gorman (2005) is of the opinion that 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.

According to Bambauer (2009a) China operates the world's most extensive and sophisticated Internet censorship system, yet rarely admits it filters information. Saudi Arabia discloses its on-line censorship and elucidates its underlying rationales. The Chinese filtering apparatus is multi-layered. 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 often considered as a country with harsh controls and therefore it is not surprising that use of the Internet is censored here. 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. Moreover, government disruption of social networking sites such as Facebook further impedes the ability of Iranians to share information and to organize protests. Furthermore, the government has conducted surveillance on Internet communications, and that surveillance may have contributed to the arrests of dissidents (Calingaert, 2010).

Censorship at varying levels is occurring in various countries hence there is abundant literature on censorship in specific countries. Examples include 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 Internet café censorship in 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) that give a picture of global censorship. Another informative study at global level covering various countries was done by Electronic Frontiers Australia (2002). Warf (2011) equally offers a comprehensive review of Internet censorship which addresses dimensions of Internet censorship and outlines levels of severity of Internet censorship across the globe. Warf (2011) classifies countries' censorship as:

- **Worst Internet censors** with examples: China, Burma/Myanmar, Vietnam and Iran.
- **Severe Internet censors** with examples: Russia, Belarus, Pakistan, Arab World countries such as Saudi Arabia, Jordan, Bahrain, etc.
- **Moderate Internet censors** with examples: Thailand, Malaysia, Singapore, Indonesia, India, Central Asia, United Arab Emirates, Sub Saharan Africa and Latin America.
- **Light Internet censors** with examples: some Latin America countries, Southern and Eastern Europe.

- **Uncensored Internet** with examples Western Europe and USA. (For the latter it might be that there are other forms of implied censorship not noted.)

7. FORMS OF INTERNET CENORSHIP: A BRIEF LITERATURE REVIEW

The new tools and techniques for controlling use of the Internet that are emerging 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 (*Access controlled*, 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).

Grothoff *et al*. (2003:1) note that Internet censorship is a “weapon” used to suppress the dissemination of information and to stifle dissent. They noted that censorship on the Internet could be done in a number of ways including filtering and denial-of-service attacks, as well as through harassment of those who publish information online (i.e. through fear) (Grothoff *et al*., 2003).

A very comprehensive review of tools and technology for Internet filtering is outlined by Murdoch and Anderson (2008) and ranges from technical filtering to domain deregistration and denial-of-service attacks. In addition, they also briefly discuss surveillance and non-technical censorship methods. Murdoch and Anderson (2008: 59-65) articulate the following filtering mechanisms:

- **TCP/IP header filtering**: With this method, 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**: This is a similar method to header filtering except that the censor’s router inspects the packet contents for any patterns or keywords that may be blacklisted. The focus is not on content, but rather 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 they can monitor all traffic that goes through them. Such a method is more powerful than TCP/IP header 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 the host server. Such attacks are usually done by having a large number of computers requesting service from a particular server and hence, overwhelming it with too much traffic which causes 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 are another form of social censorship. Families that place the computer in the living room to enable monitoring of their children's use of the Internet is another example of a social technique of censorship.

Zittrain and Palfrey (2008a:2) introduce Internet technical filtering; and define filtering as the "technical blockage of the free flow of information across the Internet". They complement the work of Murdoch and Anderson (2008) by describing in greater detail the legal and social measures used in Internet censorship such as self-censorship, which is practised by online discussion forum moderators, who often remove contributions that could lead to the blocking of their websites.

Another form of filtering is revealed by Bailey and Labovitz (2011) in the context of e-commerce. This is whereby filtering is done for purposes of engineering or commercial goals and to gain economic advantage, realize profits, or assure the availability of a resource. This can be done by blocking, limiting peer-to-peer (P2P) or Skype. According to Bailey and Labovitz (2011) a variety of techniques are employed to implement these goals (e.g., filtering URLs or packet filtering). In addition, there is a trend of large-scale censorship that co-opts the core Internet infrastructure. In this form of censorship, weaknesses in underlying routing, naming, and transport protocols are employed to perform a censorship by blocking specific classless Internet-domain routing (CIDR) addresses or autonomous system numbers (ASNs), blocking specific destinations by name, or violating the confidentiality or integrity of end-to-end communication (Bailey & Labovitz, 2011).

IP address filtering and domain name system poisoning both need government-compiled or blacklists of servers that should be blocked. Given the speed at which new content appears on the Internet, this is a time-consuming process (Murdoch & Anderson, 2008). A third option is for 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). Search engines have also been pressured by China to filter search results that contain certain keywords such as “free Tibet” (OpenNet Initiative, 2004). Deployed in this fashion, the quantity of pages blocked by keyword filters is unlikely to be acceptable outside totalitarian states. However, they can also be used to block access to specific web pages (rather than entire websites, as with IP address filtering and domain name system poisoning). This type of filtering is much more resource intensive than IP address filtering. Keyword filters in routers can be circumvented using proxies that encrypt data sent back to the requesting user, avoiding their detection (Feamster *et al*., 2002). Clayton, Murdoch and Watson (2006) also found that the specific mechanism used in Chinese networks to block access to pages based on keywords could simply be ignored by Web browsers and servers. Hybrid filtering systems have been developed that combine one or more of the filtering techniques described above. British Telecom’s “Cleanfeed” system redirects requests for web pages on a list of specific servers to a keyword filter that blocks access to specific web pages hosted on those servers. This combines the efficiency of IP address filtering with the precision of keyword filtering applied to specific pages. However, Clayton (2005) showed that the British Telecom system could be used to search out child pornography contained in pages on the secret filtering list (Brown, 2008).

Similarly, Zittrain and Palfrey (2008a:2) focused on the technical filtering aspect of Internet censorship. They defined filtering as the “technical blockage of the free flow of information across the Internet”. They also complemented the work of Murdoch and Anderson (2008) by describing in greater detail the legal and social measures used in Internet censorship. One of such measures they identified was self-censorship, which is practised by online discussion forum moderators, who often remove contributions that could lead to the blocking of their websites (Zittrain & Palfrey, 2008b:42).

Filtering is the focal point of a significant number of studies (e.g. Deibert, 2003; Heins, Cho & Feldman, 2006; Zittrain & Edelman, 2003). Other studies, on the other hand, focus 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).

Hersberger (2004) presented several mechanisms of Internet censorship, including the use of filtering software, which can block websites from access by Internet users on a certain level. Filtering can take place on the computer level or on an intranet level through network administrators and Internet service providers, in which case, only the portion of users who connect to the Internet through those layers will not be able to view the content (Hersberger, 2004: 266). If the state monopolizes all Internet service providers, then censorship would be on a national level. Filtering is the most common method used by Internet service providers to implement technical Internet censorship and what those against censorship are trying to side-step.

A growing number of countries worldwide are imposing mandatory requirements on Internet service providers to prevent their subscribers from accessing overseas content that would be banned under local laws. It is well known that undemocratic states such as China implement online censorship; but a number of democracies with constitutional guarantees of freedom of expression are also imposing digital filters. Some countries have further put pressure on Web publishers to remove content hosted outside their jurisdiction (Anderson, 2008).

According to Deibert and Villeneuve (2005), Internet censorship in countries vary in terms of the types of content blocked and (to a lesser extent) the technologies used. Such that 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, 2003).

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 much stronger where they deem it necessary or where it suites there purposes.

8 DATA MINING

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, Lybia, 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 on the *status quo* and intricacies of Internet censorship in each country with special reference to the selected trends and is intended as exemplars only.

To mine data on Internet censorship in these countries, resources of potential value were identified (See Appendix A) and searched for the name of the country; if too many references were retrieved, the name of the country was combined with search terms such as ”Internet”, “Internet censorship”, “Internet filtering” or censorship. References were manually selected. Not all web information resources used for the mining were of equal value. Sometimes websites were not available, other times references were not relevant to the topic of Internet censorship, and sometimes references were already known.

The web resources identified for searching were categorised as follows: (1) expert monitoring sites, (2) search tools specialising in news such as news search engines, and (3) meta sites, such as Browsys.com. Each country report will contain a discussion of selected trends as these manifested for the specific country, properly contextualised and referenced (See Appendix B).

Based on the literature review two categories of trends were selected for discussion, namely negative and positive trends. Negative trends include: trends in issues of Internet related privacy; ubiquitous society and control; trends in Internet related media being censored; trends in filtering and blocking Internet content (including 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 use of the Internet and trends in government models regarding Internet censorship; tends in new forms of Internet censorship; trends in support for Internet censorship; trends in enforcing regulations and Internet censorship; and trends in Internet related communication surveillance. Positive trends include: trends in reactions to Internet censorship; attempts and means to side-step e-censorship; trends in cyber actions against Internet censorship; and trends in innovative ways of showing opposition to Internet censorship. (Detail on the trends as applying to the selected countries can be found in Appendix B.) Herewith only summaries of issues of Internet censorship noted for the countries overall, as well as on the trends overall.

8.1 Brief country overview of Internet censorship based on data mining

Impressions on what is happening with regard to Internet censorship in each of the countries are influenced by what could be traced through data mining. This clearly means that not all incidents were noted and that the country reports as well as this overview reflects only partial insight – but sufficient to note reasons for concern, and to trigger further research. 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 and homosexuality are 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 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 on 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 & 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. Some countries such as Myanmar and 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 very limited effect on positioning the population of the country to benefit from the advantages of the Internet.

Detailed discussions of the selected countries are offered in Appendix B. The following table offers a brief reflection on the main impressions on each country.

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 like in other countries such as China and Myanmar. Various legislation supporting censorship and especially protection on pornography and child pornography is in place; these seems to be differing 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 relies on the arbitrary views of a judge, and equipment such as hard drives to be destroyed in cases where people were held in police custody have been noted. 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 not possible 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. These include 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. However, it seems to be affected by terrorism incidents in other countries such as Norway to steepen up measures on surveillance. Concerns have been noted that Finland 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 opinion 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 nevertheless 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 conflict, 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 to 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. Like in many other countries, the actual scope of censorship, however, seems wider, e.g. websites with negative information on Mustafa Kemal Atatürk (considered as the father of modern Turkey by many) being blocked. Concerns on violation of individual privacy did not quite feature in the data mined. Turkey uses a centralised 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 and 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 has 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.

8.2 Brief overview of trends in Internet censorship based on Internet data mining

With regard to the trends monitored, most information was 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 captured in the reports for the selected countries and are presented in Appendix B. The following table 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.

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. not even being able to send anonymous emails, and government security infiltration of 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 were noted, but limited reports on reactions to invasion of privacy were picked up through data mining.
Ubiquitous society and	Various bodies are involved in control, ranging from governments and bodies of

control	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 was 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 occurs. 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, 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 and copyrights. Some countries, e.g. Singapore, claim to rather focus on educating and preparing the general population to act 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 especially democratic countries such as the United Kingdom a strong trend towards nation-wide surveillance was noted. Very heavy surveillance in China, Mynamar (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 Mynamar 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 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.

9. 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 and 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 from 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 beh aviour. Furthermore, research on Internet censorship and the ethos of information ethics is also crucial.

10. 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. & Altiparmak, K. (2008). Internet: restricted access: a critical assessment of Internet content regulation and censorsip in Turkey. Retrieved March 3, 2012, from: http://privacy.cyber-rights.org.tr/?page_id=256
- 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. Retrieved March 26, 2012, from http://spectrum.ieee.org/telecom/internet/internet-censorship-as-bad-as-you-thought-it-was.
- Ang, P. & Nadarajan, B. (1996). Censorship and the Internet: a Singapore perspective. *Communications of the Association for Computing, 39*(6), 72-78.
- Bailey, M. & Labovitz, C. (2011). Censorship and co-option of the Internet infrastructure. Technical Report, CSE-TR-572-11. Retrieved March 06, 2012, from http://nsrg.eecs.umich.edu/publications/CSE-TR-572-11.pdf.
- 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. & Hamilton, S. (2009). Third meeting of the Internet Governance Forum (IGF), Hyderabad, India. *IFLA Journal*, *35*(1), 59-62.
- Brown, I. (2008). Internet censorship: be careful what you ask for. Retrieved 06 February 2012, from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1026597
- Calingaert, D. (2010). Authoritarianism vs Internet. *Policy Review*, *160*, 63-75.
- Clayton, R. (2005). Failures in a hybrid content blocking system. Retrieved February, 16, 2012, from http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf.
- Clayton, R., Murdoch, J. & Watson, N.M. (2006). Ignoring the Great Firewall of China. *I/S: A Journal of Law and Policy*, *3*(2), 271-296. Retrieved, February 16, 2012, from http://www-lvs12.net.ohio-state.edu/V03I02/Clayton_Formatted.pdf
- 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. & Jeapes, B. (1995). The Internet and government censorship: the case of Israeli secret. In: Proceedings of International Online Information Meeting No19, London, 5-7 December 1995 . Retrieved March 20, 2012, from http://cat.inist.fr/?aModele=afficheN&cpsidt=3151446
- Deibert, R. (2003). Black code: censorship, surveillance and the militarisation of cyberspace. *Millennium - Journal of International Studies, 32*(3), 501-530.

- Deibert R. & Villeneuve, N. (2005). Firewalls and power: an overview of global state censorship of the Internet. In: Klang, M. & Murray, A. (eds), *Human Rights in the Digital Age*. Portland, Or.: GlassHouse.
- Deibert, J. G., Palfrey, R., Rohozinski, R. & 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. & 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. & Zittrain, J. (eds.) (2012). *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*. Cambridge, MA: MIT Press.
- Deibert, R. & 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). Retrieved February 12, 2012, from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1390/1308.
- Dick, A.L., Oyieke, L.I. & Bothma, T.J.D. (2012). Are established democracies less vulnerable to Internet censorship than authoritarian regimes?: The social media test.
- 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. & 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 & policy around the world. Retrieved January 26, 2012, from https://www.efa.org.au/Issues/Censor/cens3.html.
- Faris, R. & Villeneuve, N. (2008). Measuring Global Internet Filtering. In: Deibert, J.G. *et al*. *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. Retrieved March 03, 2012 from http://static.usenix.org/event/sec02/feamster/feamster_html/.
- 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, C. *et al*. (2003). *An Encoding for Censorship-Resistant Sharing*, Technical report. Retrieved February 06, 2012, from http://www.cs.helsinki.fi/u/jtlindgr/stuff/ecrs.ps.

- Hadfield, A. (ed.). (2001). *Literature and Censorship in Renaissance England.* Hampshire: Palgrave.

- Heins, M., Choc, C. & 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. pp. 264-274.

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

- 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 the Internet censorship. *Signum*. Retrieved February, 04, 2012, from http://www.ojs.tsv.fi/index.php/signum/article/download/4397/4107.

- Lawson, T. & Comber, C. (2000). The Internet and schools: a new moral panic? *The Curriculum Journal, 11*(2), 273-285.

- 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.

- Merrett, C. (1994). *A Culture of Censorship: Secrecy and Intellectual Repression in South Africa.* Cape Town: David Philip.

- Munro, C.R. (1979). *Television, Censorship and the Law*. Aldershot: Gower Publishing Company.

- Murdoch, S.J. & 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. Retrieved January 25, 2012, from http://opennet.net/bulletins/005/.

- 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. & 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://en.wikipedia.org/wiki/Internet_censorship.

- Zittrain, J. & Edelman, B.G. (2003). Internet filtering in China. *IEEE Internet Computing*, March/April, 69-77. doi:10.2139/ssrn.399920.

- Zittrain, J. & 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. & 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.

- Zittrain, J. & Edelman, B. (2003). *Internet filtering in China.* Harvard Law School. Research Paper No. 62. Retrieved February 16, 2012, from http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan011043.pdf.

APPENDIX A: RESOURCES FOR DATA MINING

(1) Meta sites & directories

Beaucoup!	http://www.beaucoup.com
Browsys.com	http://www.browsys.com
IPL2	http://ipl2.org
The WWW Virtual Library	http://vlib.org
Yahoo directory (Internet censorship)	http://dir.yahoo.com/

(2) Search tools specialising in news such as news search engines, conventional search engines specialising in news, news services, news hubs and newspapers

Association for Progressive Communications	http://www.apc.org
BBC News	http://www.bbc.co.uk
CNN	http://edition.cnn.com/
Daily Earth	http://dailyearth.com
Global Internet Freedom Consortium	http://www.internetfreedom.org
Google news	http://news.google.com http://news.google.com/archivesearch
Guardian	http://www.guardian.co.uk/technology/internet+world/censorship
Headline Spot	http://www.headlinespot.com/
News Now	http://newsnow.co.uk
Newstrawler	http://www.newstrawler.com
Orange News	http://web.orange.co.uk/p/news/home
Platform for Internet Content Selection (PICS)	http://www.w3.org/PICS/
Sky News	http://news.sky.com/skynews/
WorldNews	http://www.wn.com
Yahoo! News	http://news.search.yahoo.com/news

(3) Expert monitoring sites

ALA	http://lists.ala.org/sympa/arc/ifaction http://lists.ala.org/sympa/arc/ifforum
Amnesty International	http://www.amnesty.org/
CIA	https://www.cia.gov/library/publications/the-world-factbook/index.html
Citizens Internet Empowerment Coalition	http://www.ciec.org
Court cases, etc.	http://www.acla.org/free-speech/internet.censorship
Electronic Frontiers Australia	http://www.efa.org
European Digital Rights	http://www.edri.org/
FAIFE Discussion list	http://infoserv.inist.fr/wwsympa.fcgi/arc/faife-l
Fifth Estate Project at Oxford Internet Institute (OII)	http://www.oii.ox.ac.uk/research/projects/?id=57
Freedom House	http://www.freedomhouse.org
Human Rights Watch	http://www.hrw.org/
IFEX	http://www.ifex.org/
Index on Censorship	http://www.indexoncensorship.org/
Internet World Stats	http://www.internetworldstats.com
OpenNet Initiative	http://opennet.net/research/profiles/
Reporters Without Borders	http://en.rsf.org/
Transparency International	http://www.transparency.org/
UNESCO Division for Freedom of Expression, Democracy and Peace	http://www.unesco.org/new/en/communication-and-information/freedom-of-expression/
World Summit on the Information Society	http://www.itu.int/wsis/index.html

APPENDIX B: COUNTRY REPORTS

1. AUSTRALIA

1.1 INTRODUCTION

Australia maintains some of the most restrictive Internet policies of any Western country and is considered by Reporters Without Borders as a potential 'Enemy Of The Internet' due to its strict Internet laws and censorship (http://www.lifehacker.com.au/2012/03/australia-still-a-potential-enemy-of-the-internet/). As a result, comparisons with China have even been noted, with reference to the "Great Australian Firewall" and "Firewall Australia" (http://en.wikipedia.org/wiki/Internet_censorship_in_Australia#Proposed_future_legislation_.28mandatory_filtering.29).

Internet censorship in Australia will be discussed under negative as well as positive trends. The discussion is based on mining a wide variety of Internet resources. There may be many more trends than noted here, as well as many more examples of each.

1.2 NEGATIVE TRENDS

1.2.1 Trends in issues of Internet related privacy

Incidents affecting Internet related privacy include steps toward a nationwide mandatory Internet filtering scheme (http://opennet.net/research/regions/australia-and-new-zealand), and a police investigation (following complaints from the public) of Google for possibly breaching privacy while taking pictures for its Street View service. Google admitted that in the processes, personal data from some unencrypted Wi-Fi services were gathered. In Australia this is considered a breach of telecommunications privacy legislation (http://www.bbc.co.uk/news/10249091).

1.2.2 Ubiquitous society and control

Internet censorship in Australia is enforced by various means such as the Australian Communications and Media Authority (ACMA). Among other things, ACMA enforces content restrictions on Internet content hosted within Australia, and maintains a "blacklist" of overseas websites which is then provided for use in filtering software (http://en.wikipedia.org/wiki/Internet_censorship_in_Australia). Already in 2009, the Australian Federal Government has been reported to organise tests for Internet filtering technology. The intention was for the filters to block access to all content on a blacklist of sites which targets material such as child pornography and depictions of sexual violence (http://www.abc.net.au/news/2009-02-27/senate-poses-tough-hurdle-for-internet-filtering/1603944). In the past there have even been reports of the Australian Government requesting a page linking to a link to allegedly harmful content to be removed (http://www.theregister.co.uk/2009/05/07/oz_link_ban/).

1.2.3 Trends in Internet related media being censored

The Australian Federal Government targets a variety of media and groups. This includes blocking websites for gamers and websites hosting and selling video games that are not suitable for 15 year olds (http://www.smh.com.au/digital-life/games/web-filters-to-censor-video-games-20090625-cxrx.html#ixzz1s0dqCcUv; http://www.smh.com.au/digital-life/games/web-filters-to-censor-video-games-20090625-cxrx.html). In 2006 a discrepancy was reported between films and computer games. At the time it seemed that films deemed suitable only for adults could be legally sold in Australia, whilst computer games of a similar nature are banned (http://www.efa.org.au/2006/02/17/computer-game-ban-highlights-need-for-censorship-reform/).

1.2.4 Trends in filtering and blocking Internet content and blocking software

Internet Service Provider (ISP) filtering is a key component of the Australian Government's plan for cyber safety. Internet service providers are expected to take some responsibility to enable the blocking of unsafe, harmful or illegal content as well as conduct on the Internet with a special focus on guidelines for child online protection and child pornography images (http://www.dbcde.gov.au/online_safety_and_security/cybersafety_plan/internet_service_provider_isp_filtering). This includes two key Internet service providers, Telstra and Optus (http://www.indexoncensorship.org/2011/07/australian-internet-providers-employ-censors/). According to a report in 2011, Australian Internet service providers will employ censors to voluntarily block websites deemed by the Government to show and disseminate child pornography. Those who attempt to access blacklisted websites will be redirected to the website of the International Criminal Police Organisation. Seemingly, accessing blacklisted websites is a criminal offence in Australia as one can be fined $11,000 a day just for linking to a blacklisted website (http://www.nocleanfeed.com/learn.html).

According to Wikileaks, some gay and straight porn websites, fringe religious groups, and Wikipedia sites are amongst the blacklisted websites (http://www.indexoncensorship.org/tag/internet-censorship/). Webpages that have been blocked include the website with the Danish government's secret index of banned child porn websites as well as Wikileaks' press release about how the index was used and why the website was publishing it. In 2008, guidelines for Internet service providers Content Filtering Pilot Technical Testing Framework were reported stating what the Australian Government expected from the Internet service providers (http://arstechnica.com/tech-policy/news/2008/12/australias-internet-filtering-too-ambitious-doomed-to-fail.ars). In 2008, the Government also announced plans for a layered filtering scheme, proposing a mandatory filter to block pornographic and illegal content, as well as an opt-out filter that would block even more content (http://opennet.net/research/regions/australia-and-new-zealand).

Similar to China, the Government decides which websites will be blacklisted under "refused classification" (http://www.prisonplanet.com/death-of-the-internet-unprecedented-censorship-bill-passes-in-uk.html). More Information on the Refused Classification (RC) material on the extensive Australian Communications and Media Authority (ACMA) list can be found at (http://www.dbcde.gov.au/online_safety_and_security/cybersafety_plan/internet_service_provider_isp_filtering; http://www.dbcde.gov.au/__data/assets/pdf_file/0006/89160/technical-testing-framework.pdf). Guidelines on the levels and definitions of prohibited content can be found at an OpenNet Initiative website (http://opennet.net/research/regions/australia-and-new-zealand).The classification system chosen for Internet content is the more restrictive standard used for films, rather than the publications classification. As a result, some content allowable offline is banned when brought online (http://opennet.net/research/regions/australia-and-new-zealand). Thus even web-based games deemed unsuitable for anyone over the age of fifteen will be blocked.

In addition, the use of a wide variety of personal computer (PC)-based (end user) filters have been reported such as IIA Family Friendly Filters, AOL Parental Control (PC-based software communicates with AOL's server-based filtering system), Arlington Custom Browser, Cyber Patrol, Cyber Sentinel, Cybersitter, Net Nanny, Norton Internet Security (http://www.efa.org.au/Issues/Censor/cens2.html#reviews).

1.2.5 Trends in technologies to monitor and identify citizens using the Internet to express their opinion and applying "freedom of speech"

The Internet Industry Association (IIA) is Australia's national Internet industry organisation (http://www.iia.net.au) responsible for the Industry Content Code of Practice which includes the "scheduled" filters used in Australia and registered by the ACMA. The Code applies to all Australian Internet service providers and the ACMA has powers to enforce compliance (More information is available at http://www.efa.org.au/Issues/Censor/cens2.html#reviews).

1.2.6 Criminalization of legitimate expression (e.g. thoughts, ideas, arguments) on the Internet

Some legislation and incidents of criminalisation have been reported. Electronic Frontiers Australia reported on the New South Wales (NSW) law that would criminalise Internet material unsuitable for children. The law will cover text and images placed on the web, including email sent to mailing lists that are archived on the Web, and messages to newsgroups (http://www.efa.org.au/Publish/PR011117.html). In

May 2011 the International Federation of Journalists (IFJ) expressed concern about the arrest of a journalist and seizing of his iPad after he reported on a security flaw on the popular social networking service Facebook. The journalist was released a short time later, but the iPad was held by police (http://www.ifex.org/australia/2011/05/19/grubb_arrested/). Concern about the press freedom implications of the proposed Australian legislation that would give the federal police commissioner powers to unilaterally block Internet content that he or she "has reason to believe . . . is crime or terrorism related" has in fact been raised for quite some time (http://www.ifex.org/australia/2007/10/10/proposed_new_legislation_empowering/).

In 2009 the Australian Internet company, auDA that runs the *.com.au* domain registry has been accused of censoring a website satirising Australian Communications Minister Stephen Conroy's proposed Internet censorship laws (http://www.indexoncensorship.org/2009/12/australia-anti-censorship-website-censored/).

1.2.7 Trends in acts, regulations and legislation regarding use of the Internet or trends in government models regarding Internet censorship

Already in 2003, the Australian Internet Industry Association (IIA) attempted to establish a code of practice requiring Internet service providers to retain user information for six or twelve months and provide it to law enforcement upon official request. Specifically, personal data such as name, address, and credit card details were to be retained by Internet service providers for six months after a customer ends service with that Internet service provider or twelve months after the record is created, whichever is longer. Operational data, such as proxy logs and e-mail information, were to be kept for six months after creation of the data. Law enforcement could request this information using the certificate system set up in the Telecommunications Act 1997 (http://opennet.net/research/regions/australia-and-new-zealand).

The Australian Communications and Media Authority (ACMA) has the power to enforce content restrictions on Internet content hosted within Australia, and maintain a "blacklist" of overseas websites which is then provided for use in filtering software. Already since October 2008, the governing Australian Labor Party has proposed to extend Internet censorship to a system of mandatory filtering of overseas websites which falls under "refused classification" (RC) in Australia. This means that Internet service providers would be required to block access to such content for all users (http://en.wikipedia.org/wiki/Internet_censorship_in_Australia).

States and territories in Australia have instituted a variety of laws that criminalize the downloading of illegal content and the distribution of content that is ‘‘objectionable’’ or ‘‘unsuitable for minors’’ (e.g. the state of Victoria). There is, however, no uniformity between the states. An example of legislation includes the The Broadcasting Services Act 1992. The provisions of Schedule 5 and Schedule 7 of the Broadcasting Services Act 1992 inserted in 1999 and 2007 allow to effectively ban some content from being hosted within Australia. Under this regime, if a complaint is issued about material "broadcast" on the Internet the Australian Communications and Media Authority is allowed to examine the material under the guidelines for film and video (http://en.wikipedia.org/wiki/Internet_censorship_in_Australia; (http://www.efa.org.au/Issues/Censor/cens3.html#aust).

Although Australia has legislation addressing hate speech generally, and in relation to the Internet, it however does not seem to have an institutionalized investigation system in this regard (http://opennet.net/research/regions/australia-and-new-zealand).

1.2.8 Trends in new forms of Internet censorship, e.g. Halaal Internet, implied censorship such as user rating

Australia's initial attempts to filter the Internet of all "inappropriate content" and "offensive and illegal material" seemed to have turned from safeguarding children from things like child pornography to legal pornography, gambling, and even peer-to-peer (P2P) traffic, fetishy sex, instruction in crime (such as euthanasia), and computer games considered not suitable for under eighteen's. The list is partly generated by complaints from the public, and may include lists imported from overseas police departments. It is noted that the censorship push started its life as a cyber-safety policy, where Internet service providers would require to provide a filtered solution to families, but has since turned into something less useful and more sinister (http://www.efa.org.au/2009/12/17/filtering-coming-to-australian-in-2010/; http://www.smh.com.au/digital-life/games/web-filters-to-censor-video-games-20090625-cxrx.html#ixzz1sknIyWio; http://www.smh.com.au/digital-life/games/web-filters-to-censor-video-games-20090625-cxrx.html). The Australian Broadband Minister, Stephen Conroy, a main proponent of Australia's attempt at Internet citizenship, has also been reported to launch a blog to promote Australia's Cyber-Safety Plan, as well as a threat to reduce Internet connection speeds by 87% and institute a system of censorship with no oversight (http://www.zeropaid.com/news/10002/australia_internet_filtering_trial_to_begin_with_6_isps/).

Reported rating systems used with Platform for Internet Content Selection (PICS) include the RSACi Rating System covering four categories of material: sex, nudity, language and violence, and the safesurf rating system with categories for: suitable age range, profanity, heterosexual themes, homosexual themes, nudity and consenting sexual acts, violent themes, sexual violence, accusations or attacks against racial or religious groups, themes advocating or glorifying illegal drug use, other adult themes requiring parental caution, and gambling. Owing to perceived problems with the RSACi system, Electronic Frontiers Australia (EFA) has condemned the RSACi ratings system as totally unsuited to its stated objective. Cyber Patrol's CyberNOT Block List forms the basis of a third-party rating server. The client software accesses a rating server to determine the content ratings for requested material. The CyberNOT Service provides rating information on two categories, sex and other. The Sex category includes four sub-categories: gross depictions; sexual acts/text; partial nudity, nudity. The other sub-category includes: racist/ethnic; gambling; satanic/cult; drugs & drug culture; militant/extremist; violence/profanity; questionable/illegal and alcohol, beer & wine (http://www.efa.org.au/Issues/Censor/cens2a.html#rating).

1.2.9 Trends in support of Internet censorship, e.g. computer and Internet companies, search engines, Internet service providers

Examples in support of Internet censorship in Australia include NetAlarmed which checks every visit to a website NetAlarmed Data Centre in Canberra. Depending on the website's content, it is then approved or blocked to those accessing the Internet from within Australia. If a website is blacklisted you will be safe in knowing the website was not suitable for viewing. Depending on the website's content, it is then approved or blocked to those accessing the Internet from within Australia. If a website is blacklisted people know that it is not considered safe for viewing (http://www.netalarmed.com/). In-spite of concerns about the scope of Internet censorship in Australia, support for the Government's efforts and even calls for stronger action has been noted; such as calls to sharpen action against online pornography seen as a great danger for young people (http://www.efa.org.au/2010/03/11/oz-internet-censorship-noticed-in-china/). Campaigns by groups as well as individuals for government mandated Internet service provider-based filtering and blocking of web pages unsuitable for children has been reported over a number of years e.g. in 1999 by politicians within the Federal Coalition Government, in late 2004 by the Family First Party, late 2005 by the people associated with the "Sexual Integrity Forum" organised by the Fatherhood Foundation and in early 2006 by the Federal Labor Party (http://www.efa.org.au/Issues/Censor/cens2.html#reviews). Google, Yahoo and Microsoft expressed concern for the Australian Government's actions for Internet filtering since the restrictions could be applied to legitimate information on issues such as euthanasia, abortion and drug addiction, as well as media reporting on criminal activity (http://www.indexoncensorship.org/2010/10/australia-pm-backs-new-internet-filter/).

1.2.10 Trends in enforcing regulations and Internet censorship

Various means of enforcing regulations and Internet censorship have been reported amongst others a fine of AUD 11,000 per day for those who link to banned websites (http://opennet.net/research/regions/australia-and-new-zealand).

1.2.11 Trends in Internet related communication surveillance

Australia’s Internet surveillance regime is primarily based on two laws: (1) The Telecommunications (Interception and Access) Act 1979, and amended in 2006. Amongst other things it allows law enforcement to do real-time interception of telecommunications as well as access to stored telecommunications warrants (without a requirement to notify the communicants); (2) The Surveillance Devices Act 2004, which allows law enforcement to install surveillance devices such as keystroke recorders under newly created ‘‘surveillance device warrants.’’ Electronic Frontiers Australia has expressed concern that these warrants will be used by law enforcement to avoid applying for a telecommunications service warrant, essentially allowing them to intercept communications where a telecommunications service warrant would not have been authorized (http://opennet.net/research/regions/australia-and-new-zealand).

1.3 POSITIVE TRENDS

1.3.1 Trends in reactions to Internet censorship: changes in groups, group dynamics, responses and actions of groups

Electronic Frontiers Australia, a non-profit national organisation representing Internet users concerned with on-line rights and freedoms, was established in 1994, and plays an important role in opposing Internet censorship in the country e.g. through petitions against content regulation (http://www.efa.org.au/Campaigns/petn.html) and critique on the government’s actions regarding Internet censorship (http://www.efa.org.au/Publish/PR990308.html). It functions independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting online civil liberties (http://www.efa.org.au/2008/12/08/efa-welcomes-widespread-opposition-to-net-censorship/). Outburst on the social networking website, Facebook has also been reported “I DO NOT Support Australia Implementing MANDATORY Internet Censorship!!! I DO NOT Support Australia Implementing MANDATORY Internet Censorship!!!. ... Censorship to the internet is like burning thousands of libraries down, do ... Censorship and fluoride are things we must fight” (http://www.facebook.com/group.php?gid=43233359691).

Arguments for free access to the Internet, even to websites with illegal or immoral content have been noted. These include the opportunity to identify and apprehend pedophiles, and even networks of pedophiles as a result of their behaviour online (http://mcbean.hubpages.com/hub/Internet-Censorship-Australia-China).

1.3.2 Attempts and means to side-step Internet censorship (e.g. specialised software such as FREEBIRD, tracing blackouts, attempts to involve the public and public opinion)

At the time of data mining no specific trends on attempts and means to side-step Internet censorship were noted.

1.3.3 Trends in cyber actions against Internet censorship, e.g. cyber and virtual demonstrations and protest

In 2010 an attempt by a group of cyber-activists was reported to jam key Australian government websites for two consecutive days. These include the main government website (http://www.australia.gov.au) and the Australian parliament's homepage (http://www.aph.gov.au). The protest was against Internet filtering (http://news.smh.com.au/breaking-news-technology/australia-cyber-attacks-could-last-months-hackers-20100211-nuzc.html).

1.3.4 Trends in innovative ways of showing opposition to Internet censorship

Various ways of opposing Internet censorship have been noted such as criticism by Reporters Without Borders (http://www.3news.co.nz/Australia-France-internet-laws-under-fire/tabid/412/articleID/246281/Default.aspx#ixzz1sl0tnQB3), an international survey showing that the Australian public does not support government censorship of the Internet, (http://www.efa.org.au/Publish/PR990829.html), and protest rallies against the Australian Government's reported "A$70 million national clean feed Internet scheme" (http://www.itworld.com/internet/59256/australia-sees-rallies-against-internet-filtering-plan).

Other reported events include a forum on Internet Censorship entitled "Cyberhate? Censorship on the Internet" (http://www.efa.org.au/2009/09/07/tuesday-forum-on-internet-censorship-in-sydney/), a petition against censorship of Australian Internet (http://www.efa.org.au/Publish/PR970726.html), opposition against censorship laws from the political arena as well as civil society (http://www.efa.org.au/2009/04/22/melb-event-the-tangled-web-beyond-an-internet-filter/), the hacking of The Australian National Classification Board's website before Senator Stephen Conroy went onto television to defend the government's Internet filtering scheme on 29 March 2009.The hackers posted on the website that it is 'part of an elaborate deception from China to control and sheepify the nation'. The attack was, however, condemned by those working to convince the Government to abandon its trials of Internet filtering (http://www.indexoncensorship.org/2009/03/australian-%e2%80%98hacktivists%e2%80%99-attack-classification-website/#more-1876).

Google has recently urged the Australian Federal Government to reject an interim independent report recommending the country's Internet be regulated in a similar manner to television. Google is arguing for a "new independent regulator for content and communications" that is technology-neutral (http://www.indexoncensorship.org/2012/02/australia-google-urges-rejection-of-web-regulation/). In addition, The Australian Library and Information Association (ALIA) remains opposed to Internet filtering, despite concerns raised over library users caught viewing pornography (http://www.itnews.com.au/News/150669.libraries-object-to-internet-filtering.aspx). Although some opposing of the Internet related legislation in Australia has been reported, Wikipedia is of the opinion that there don't seem to be much success (http://en.wikipedia.org/wiki/Internet_censorship_in_Australia).

1.4 CONCLUSION

Although not necessarily politically or ideologically motivated, Australia is noted for stringent government control as well as input from the public regarding restricting access to certain types of information via the Internet. The scope of legislation and efforts to restrict control has been compared to Internet censorship in China, although it is certainly not marked by the same attempts to use fear and severity in punishment to enforce the legislation.

1.5 REFERENCES

http://arstechnica.com/tech-policy/news/2008/12/australias-internet-filtering-too-ambitious-doomed-to-fail.ars

http://en.wikipedia.org/wiki/Internet_censorship_in_Australia

http://en.wikipedia.org/wiki/Internet_censorship_in_Australia#Proposed_future_legislation_.28mandatory_filtering.29

http://mcbean.hubpages.com/hub/Internet-Censorship-Australia-China

http://news.smh.com.au/breaking-news-technology/australia-cyber-attacks-could-last-months-hackers-20100211-nuzc.html

http://opennet.net/research/regions/australia-and-new-zealand

http://www.3news.co.nz/Australia-France-internet-laws-under-fire/tabid/412/articleID/246281/Default.aspx#ixzz1sl0tnQB3

http://www.abc.net.au/news/2009-02-27/senate-poses-tough-hurdle-for-internet-filtering/1603944

http://www.bbc.co.uk/news/10249091

http://www.dbcde.gov.au/__data/assets/pdf_file/0006/89160/technical-testing-framework.pdf

http://www.dbcde.gov.au/online_safety_and_security/cybersafety_plan/internet_service_provider_isp_filtering

http://www.efa.org.au/2006/02/17/computer-game-ban-highlights-need-for-censorship-reform/

http://www.efa.org.au/2008/12/08/efa-welcomes-widespread-opposition-to-net-censorship/http://www.facebook.com/group.php?gid=43233359691

http://www.efa.org.au/2009/04/22/melb-event-the-tangled-web-beyond-an-internet-filter/

http://www.efa.org.au/2009/09/07/tuesday-forum-on-internet-censorship-in-sydney/

http://www.efa.org.au/2009/12/17/filtering-coming-to-australian-in-2010/

http://www.efa.org.au/2010/03/11/oz-internet-censorship-noticed-in-china/

http://www.efa.org.au/Campaigns/petn.htmlhttp://www.efa.org.au/Publish/PR990308.html

http://www.efa.org.au/Issues/Censor/cens2.html#reviews

http://www.efa.org.au/Issues/Censor/cens2a.html#rating

http://www.efa.org.au/Issues/Censor/cens3.html#aust

http://www.efa.org.au/Publish/PR011117.html

http://www.efa.org.au/Publish/PR990829.html

http://www.ifex.org/australia/2007/10/10/proposed_new_legislation_empowering/

http://www.ifex.org/australia/2011/05/19/grubb_arrested/

http://www.iia.net.au

http://www.indexoncensorship.org/2009/03/australian-%e2%80%98hacktivists%e2%80%99-attack-classification-website/#more-1876

http://www.indexoncensorship.org/2009/12/australia-anti-censorship-website-censored/

http://www.indexoncensorship.org/2010/10/australia-pm-backs-new-internet-filter/

http://www.indexoncensorship.org/2011/07/australian-internet-providers-employ-censors/

http://www.indexoncensorship.org/2012/02/australia-google-urges-rejection-of-web-regulation/

http://www.indexoncensorship.org/tag/internet-censorship/

http://www.itnews.com.au/News/150669.libraries-object-to-internet-filtering.aspx

http://www.itworld.com/internet/59256/australia-sees-rallies-against-internet-filtering-plan

http://www.lifehacker.com.au/2012/03/australia-still-a-potential-enemy-of-the-internet/

http://www.netalarmed.com/

http://www.nocleanfeed.com/learn.html

http://www.prisonplanet.com/death-of-the-internet-unprecedented-censorship-bill-passes-in-uk.html

http://www.smh.com.au/digital-life/games/web-filters-to-censor-video-games-20090625-cxrx.html#ixzz1s0dqCcUv

http://www.smh.com.au/digital-life/games/web-filters-to-censor-video-games-20090625-cxrx.html

http://www.smh.com.au/digital-life/games/web-filters-to-censor-video-games-20090625-cxrx.html#ixzz1sknIyWio

http://www.theregister.co.uk/2009/05/07/oz_link_ban/).

http://www.zeropaid.com/news/10002/australia_internet_filtering_trial_to_begin_with_6_isps/

2. CHILE

2.1 INTRODUCTION

Although data mining could trace reports on television and other media censorship in Chile (http://en.rsf.org/chile.html?debut_contenu=8), not much could be traced on Internet censorship. It might be that such reports are in Spanish, which was not considered due to language constraints. In Chile, there is a strong relationship between politics and censorship and it seems as if, especially the Chilean Socialists are very active in this regard. This is not only with regard to what is available on the Internet, but also in public speech which differs from their ruling party opinions. This is evident from the efforts of Chilean senator Isabel Allende (http://www.allchile.net/chileforum/topic4175-12.html). Some reports, however, indicate that censorship in Chile is more in line with trends in Northern America and European countries, such that it focuses on child pornography and restricts child access to age-inappropriate material (http://opennet.net/research/regions/la).

Internet censorship in Chile will be discussed under negative as well as positive trends. The discussion is based on mining a wide variety of Internet resources. There may, however, be many more trends than noted here, as well as many more examples of each. Each individual trend might also be mined in more depth to give a true reflection for the country.

2.2 NEGATIVE TRENDS

2.2.1 Trends in issues of Internet related privacy

At the time of data mining, specific incidents related to Internet privacy were not noted.

2.2.2 Ubiquitous society and control

At the time of mining data, specific reports on ubiquitous society and control was not noted.

2.2.3 Trends in Internet related media being censored

Data mining did not deliver specific information about the spectrum of media being monitored. What was interesting to note is a report indicating that in case of detentions (even short detentions), people's equipment is destroyed which according to the report amounts to censorship since it discourages journalists to hold interviews and gather information (http://en.rsf.org/chile-aysen-protests-and-student-rallies-19-03-2012,42158.html).

2.2.4 Trends in filtering and blocking Internet content and blocking software

With the exception of Cuba, a systematic technical filtering of the Internet is not well established in Latin America, including Chile. Currently the regulation of Internet content seems to be rather similar to the trends (concerns and strategies followed) in North America and Europe. The focus is on combating the spread of child pornography and restricting child access to age-inappropriate material. As Internet usage in Latin America increases, so have defamation, hate speech, copyright, and privacy issues (http://opennet.net/research/regions/la).

Some incidents of hacking news websites and even the bombing of a newspaper publisher (Copesa, publisher of the daily La Tercera) have been reported (http://en.rsf.org/chile.html), as well as removal of the hard disks from computers belonging to a newspaper (http://en.rsf.org/chile.html?debut_contenu=8). Following such incidents, a Reporters Without Borders report stated the following concerns: “All the Chilean media, both alternative and traditional, are threatened by these online attacks on three news websites and the homemade bomb attack on Copesa”… “This climate of violence must be checked by police and judicial action and by a political response to the public’s calls for media pluralism. A broad debate involving all of society cannot be put off any longer. Otherwise the situation will keep deteriorating and there will be a dangerous increase in intolerance and polarization” (http://en.rsf.org/chile-three-news-websites-hacked-10-11-2011,41375.html).

2.2.5 Trends in technologies to monitor and identify citizens using the Internet to express their opinion and applying “freedom of speech”

At the time of mining data, reports on trends on technologies to monitor and identify citizens using the Internet to express their opinion were not noted.

2.2.6 Criminalization of legitimate expression (e.g. thoughts, ideas, arguments) on the Internet

Some concerns were noted with regard to the destruction of people’s equipment, removal of hard disks, and judges deciding on the interpretation of behaviour in accordance with legislation which is quite vague in referring to issues such as “proper customs” (http://www.isoc.org/inet2000/cdproceedings/8k/8k_4.htm; http://en.rsf.org/chile.html?debut_contenu=8; http://en.rsf.org/chile-aysen-protests-and-student-rallies-19-03-2012,42158.html)

2.2.7 Trends in acts, regulations and legislation regarding use of the Internet and trends in government models regarding Internet censorship

At the time of mining data, reports on trends in acts, regulations and legislation only picked up a reference to a proposal for a Bill to censor the contents of the Internet e.g. a Bill reported in 2000 proposing to punish individuals that use the Internet to disseminate contents that are offensive to morals, public order or "proper customs." Such a Bill can be interpreted as a "blank penal law", because the determination of whether a given conduct is contrary to the law is in the hands of the judge. It is for the judge to decide if given behaviour is against what is understood to be "morally correct," or if it belongs to the realm of the private, and therefore outside of the interest of the general community. It is also the judge who determines if something is against "proper customs" (http://www.isoc.org/inet2000/cdproceedings/8k/8k_4.htm).

Although numerous groups in Chile have recommended legislation to make access to the Internet a right, alongside access to clean water and shelter, the high value placed on Internet access has been reported not yet to have resulted in uniformly unfettered access (http://opennet.net/research/regions/la**).**

2.2.8 Trends in new forms of Internet censorship, e.g. Halaal Internet, implied censorship such as user rating

At the time of mining data, no reports on trends in new forms of Internet censorship were noted.

2.2.9 Trends in support of Internet censorship, e.g. computer and Internet companies, search engines, Internet service providers

At the time of mining data, no reports on trends in support of Internet censorship were noted.

2.2.10 Trends in enforcing regulations and Internet censorship

In Chile, the right of access to information is protected by the 2008 Transparency and Access to Information Act. It seems as if the Council for the Transparency of Chile has been shown to be effective as an appeal body in this regard. Civil society monitoring of resistance, however, still finds ignorance of this Act by officials (http://www.freedominfo.org/2011/06/report-analyzes-access-in-7-latin-american-countries/). Some of the legislation in Chile affecting Internet censorship includes the Faults Administration of Freedom of Information (FOI) Law and the Transparency Act.

As for access to information, attempts to improve access to information and requesting information are however reported. In 2011 e.g. a study conducted on 169 organisations identified problems with using the Internet to make requests for information. It found that only 47% of the time could applications be made via the Internet. In addition 71% of the requestors faced problems with the electronic systems (http://www.freedominfo.org/2011/05/study-in-chile-faults-administration-of-foi-law/). Following this, some plans were made to improve access: on April 15 2011, the Council for Transparency (*Consejo para la Transparencia*) and the General Secretariat of the Presidency signed an agreement to develop a Transparency Web Portal. The Transparency Web Portal is intended as a one-stop shop where access to information requests can be made electronically to all Chilean authorities subject to Law 20.285 on Transparency and Access to Information. People will be able to follow up on the status of their requests. Once the portal is accessible to the public, the *Consejo* will be able to gather important statistical information on compliance to requests (http://www.freedominfo.org/2011/04/chile-plans-to-create-transparency-web-portal/).

2.2.11 Trends in Internet related communication surveillance

At the time of mining data, no trends on Internet related communication surveillance were noted.

2.3 POSITIVE TRENDS

At the time of data mining, nothing specifically relating to trends in reactions to Internet censorship: changes in groups, group dynamics, responses and actions of groups, attempts and means to side-step e-censorship, or trends in cyber actions against Internet censorship, were noted.

2.3.1 Trends in innovative ways of showing opposition to Internet censorship: changes in groups, group dynamics, responses and actions of groups

Some trends in showing opposition to Internet censorship were, however, noted. Chile was reported to become the first country in the world to successfully implement a law guaranteeing network neutrality (http://opennet.net/blog/2010/11/internet-filtering-latin-america). The process of deregulation has also led to a surge in more affordable and increasingly popular services such as Voice-over Internet Protocol (VoIP) (http://opennet.net/research/regions/la). In Chile the VoIP markets operate as if unregulated; In October 2006, after deregulation, Telefónica Chile was fined nearly USD1 million for antitrust violations in blocking VoIP calls.

Chile has also been reported as a leader in high-speed Internet access (http://opennet.net/research/regions/la).

At the time of data mining no reports relevant to (1) attempts and means to side-step Internet censorship, (2) trends in cyber actions against Internet censorship, and (3) trends in innovative ways of showing opposition to Internet censorship was noted.

2.4 CONCLUSION

Considering the limited amount of information that could be traced on Internet censorship in Chile it seems that although there are concerns on freedom of expression regarding tolerance for opposing views, there is no evidence of large scale attempts by the government at blocking Internet access and keeping people from using the Internet as a tool to access and disseminate information. It might be that more information on the positive as well as negative trends might be available in Spanish; this option, however, was not pursued.

2.5 REFERENCES

http://en.rsf.org/chile.html
http://en.rsf.org/chile-aysen-protests-and-student-rallies-19-03-2012,42158.html
http://en.rsf.org/chile.html?debut_contenu=8;
http://en.rsf.org/chile-three-news-websites-hacked-10-11-2011,41375.html
http://opennet.net/blog/2010/11/internet-filtering-latin-america
http://opennet.net/research/regions/la
http://opennet.net/research/regions/la
http://www.allchile.net/chileforum/topic4175-12.html
http://www.freedominfo.org/2011/06/report-analyzes-access-in-7-latin-american-countries/
http://www.isoc.org/inet2000/cdproceedings/8k/8k_4.htm

3 CHINA

3.1 INTRODUCTION

China is very strongly associated with censorship, Internet censorship and a lack of freedom of speech, and is one of the countries listed as an “Enemy of the Internet” by Reporters Without Borders (http://en.rsf.org/china-china-12-03-2012,42077.html). It is however said that “China may have the world’s most sophisticated online censorship and surveillance system, but it has been pushed to its limits to thwart any risk of contagion from protest movements” (http://en.rsf.org/china-china-12-03-2012,42077.html).

Internet censorship in China will be discussed under negative as well as positive trends. The discussion is based on mining a wide variety of Internet resources. There may be many more trends than noted here, as well as many more examples of each. Each individual trend might also be mined in more depth to give a true reflection for the country.

3.2 NEGATIVE TRENDS

3.2.1 Trends in issues of Internet related privacy

Numerous incidents have been reported on monitoring email and other forms of electronic messages, to smother any hint of anti-government sentiment. Users are required to register with an Internet service provider (ISP) when they purchase Internet access at home or at work, so that they cannot operate online anonymously. Furthermore, email is intercepted to monitor dissidents by means of deep packet inspection. This enables the state security to intercept email messages, deconstruct them, pick out keywords, remove or alter the content of these messages, and reconstruct them within milliseconds. Surveillance is also extended to cell phone calls (Calingaert, 2010; http://www.nytimes.com/2011/03/22/world/asia/22china.html?_r=1).

3.2.2 Ubiquitous society and control

Censorship of email and Internet usage and surveillance have often been reported to be outsourced to private companies such as Internet service providers, bloghosting companies, cybercafés, and mobile phone operators. Customers at cybercafés have to present identification, and cybercafés have to install software to monitor and filter customers' web browsing (Calingaert, 2010).

3.2.3 Trends in filtering and blocking Internet content and blocking software

Various incidents have been reported on the use of web-filtering technology and Internet filtering software such as Websense (http://www.websense.com/content/home.aspx) to block websites that address topics the Chinese government considers sensitive, such as the controversies surrounding the 2008 Olympics and repression of Christians in China. Such software has been reported to be used in schools and universities (Calingaert, 2010). Government computers intercept incoming data and compare it against an ever-changing list of banned keywords or websites, screening out much information. Since late 2010, the censors have prevented Google searches of the English word “freedom”, or “occupy” followed by the name of a Chinese city e.g. “Occupy Beijing” (http://en.rsf.org/china-china-12-03-2012,42077.html) as well as many other words. Websites offering access to films, video games and other forms of entertainment are also often blocked.

3.2.4 Trends in Internet related media being censored

Various electronic media types are targeted for censorship, with a strong focus on blogs. Blogs and websites are hacked or subjected to denial-of-service attacks, which disrupt or shut down the websites. State security services infiltrate online networks, monitor discussions about planned civic actions, and identify members of opposition groups. Facebook, the most widely used social networking service, allows users to create private groups but does not offer secure login. State security services therefore hacks the Facebook pages of known activists and in the process can identify the activist's entire network of friends and contacts (http://topics.nytimes.com/topics/news/international/countriesandterritories/china/internet_censorship/index.html). More recently searches for content on microblogs have been blocked to stifle mention of the "Jasmine Revolution" that was to be staged in Chinese cities in 2011 (http://www.techworld.com.au/article/377359/china_blocks_microblogs_jasmine_revolution). There are also reports of routine blocking of foreign news media, websites of political opponents, and web pages flagging up human rights abuses (http://www.bbc.com/news/technology-17476788).

3.2.5 Trends in acts, regulations and legislation regarding use of the Internet and trends in government models regarding Internet censorship

Citizens of China are limited in their ability to set up personal websites and to view hundreds of websites offering films, video games and other forms of entertainment (http://www.nytimes.com/2009/12/18/world/asia/18china.html?_r=1&ref=internetcensorship). The Government requires manufacturers to install Internet filtering software on all new computers. These are called Green Dam Youth (http://en.wikipedia.org/wiki/Green_Dam_Youth_Escort). Individuals are also banned from registering websites ending in .cn, China’s country code domain name. Websites are also shut down; a New York Times news clip reported in 2009 that more than 700 websites specifically those that offer free movies, television dramas and music downloads were to be shut down (http://www.nytimes.com/2009/12/18/world/asia/18china.html?_r=1&ref=internetcensorship).

It seems as if manufacturers and consumers are not free to select filtering software and are mandated to use Green Dam, which has been described as technically flawed (http://news.bbc.co.uk/2/hi/business/8118055.stm). Although the use of Green Dam is considered mandatory, there has been virtually no public notice on this (http://news.bbc.co.uk/2/hi/business/8118055.stm).

In terms of regulation, the "Great Firewall of China" or "Golden Shield Project" stands out. Its main function is to censor and control Internet information both domestically and globally by blocking thousands of websites, including those linked to the Dalai Lama and the banned Falun Gong spiritual movement (Liang & Lu, 2010; http://www.bbc.co.uk/news/world-asia-pacific-13455819).
China has established a special Internet police force to assist its Internet surveillance (Liang & Lu, 2010). It also has a Chinese Internet Censorship Agency that promotes the creation of government regulated news websites as well as managing the government's online publicity initiatives. Furthermore, the purpose of the Agency is to investigate and punish any website owner that is violating Chinese Internet censorship laws and regulations. It oversees providers with their efforts to improve the management and handling of domain name registration, website registration, the distribution of IP addresses and Internet access (http://www.vpnhero.com/news/china-internet-censorship-getting-worst/). Beijing has been reported to have a new police regulation that requires businesses such as restaurants, bars and hotels to install costly Internet access control systems. According to Beijing police the new measures target online gambling, hackers and porn website visitors but critics say it's a new way to censor the Internet (http://www.vpnhero.com/news/china-to-monitor-public-internet-users-in-beijing/).

3.2.6 Trends in technologies to monitor and identify citizens using the Internet to express their opinion and applying "freedom of speech"

The use of filtering software such as Websense has been reported.

3.2.7 Criminalization of legitimate expression (e.g. thoughts, ideas, arguments) on the Internet

It seems as if online surveillance was stepped up over the last few years: websites were entirely or partially closed, online social networks were shut down, online news portals were censored, online journalists and bloggers were detained and arrested. It seems as if there is a trend for increased censorship (http://edition.cnn.com/2010/WORLD/asiapcf/01/31/china.censorship/index.html?iref=allsearch).

Numerous incidents of the intimidation of bloggers and online journalists have also been noted. According to Reporters Without Borders "Arbitrary detentions, unfair trials, repressive regulations and harsh sentences have recently multiplied, taking special aim at cyber-dissidents. Seventy-eight of them are still in jail for their online activities, making China the world's biggest prison for netizens. Victims include: Nobel Peace Prize winner Liu Xiaobo, who is still behind bars and cyber-dissidents Chen Xi and Chen Wei**, and** Li Tie **(**http://en.rsf.org/china-china-12-03-2012,42077.html).

At the time of data mining information on the following trends were not noticed: (1) trends in new forms of Internet censorship, (2) trends in support of Internet censorship, (3) trends in enforcing regulations on Internet censorship, and (4) trends in Internet related communication surveillance. Nonetheless, in view of censorship reports on email outlined earlier, one detects Internet related communication surveillance in China.

3.3 POSITIVE TRENDS

3.3.1 Trends in reactions to Internet censorship

At the time of data mining no reports on specific trends in reactions to Internet censorship were noted.

3.3.2 Attempts and means to side-step Internet censorship

On the positive side it is noted that it has been reported to be possible to gain access to censored content through circumvention software and sharing files through peer-to-peer (P2P) networks or overseas file transfer protocol (FTP) sites. Citizens avoid government blocks on their blog posts by deliberately misspelling keywords that trigger filters or, since filters search for text, by posting their words as an image file. They also resort to allegory to criticize government repression. In China, for example, citizens have widely discussed and circulated online cartoons and videos of the mythical grass-mud horse and its struggle against the evil river crab, which symbolized Internet censorship. Secure login has also been reported for a free email service i.e. Google mail (Calingaert, 2010). Use of web proxy software, Psiphon, created by Toronto University's Citizen Lab, the Global Internet Freedom Consortium's anti-censorship software UltraSurf and FreeGate, and TOR (The Onion Router) system for anonymous online communication promoted in the public domain by the Electronic Frontier Foundation has also been noted (Calingaert, 2010).

Dynamic Internet Technology (DIT) uses a proxy network called DynaWeb to enable users to circumvent the Internet censorship in China and gain secure and full access to the Internet.

Through FreeGate, DIT's proxy network software, Internet users in China can even access forbidden websites (http://www.internetfreedom.org/files/Research/battle-for-freedom-in-chinese-cyberspace.pdf).

Microbloggers have been using cryptic code words, ranging from Teletubbies to Instant Noodles, to keep comments about Bo Xilia's dismissal and meetings of the Politburo Standing Committee of the Communist Party from being blocked. According to *The Guardian* the blog Offbeat China, has published a list of key words used by bloggers as well as a sample blog posts that incorporated the codes (http://www.editorsweblog.org/2012/03/23/overcoming-censorship-how-chinese-bloggers-are-outsmarting-the-great-firewall).

Global Internet Freedom (GIF) is a consortium formed by several technology companies that specialises in circumventing political censorship on the Internet by repressive regimes. It released software called "Green Tsunami," designed for Chinese users to detect, disable or remove "Green Dam" Firewall. The Green Tsunami gives users options to temporarily disable the monitoring of "Green Dam," or to completely purge it from their computers (http://www.internetfreedom.org/Green%20Tsunami%20Released%20to%20Burst%20Green%20Dam).

3.3.3 Trends in cyber actions against Internet censorship

At the time of data mining no reports on specific trends in cyber actions against Internet censorship were noted.

3.3.4 Trends in innovative ways of showing opposition to Internet censorship

According to Calingaert (2010) Support from the Global Internet Freedom Fund might be considered for both technological innovation and indigenous efforts in Internet-restricted countries to expand the space for free expression online. This might be an option to investigate.

3.4 CONCLUSION

China portrays some of the most severe restrictions on Internet access with regard to political, social and religious issues. The Chinese government practice a very strong control of censorship, also involving Internet service providers and other components of society. Although some counter actions are reported, the perception is that it has only a very limited impact on freedom of access to information and freedom of expression.

REFERENCES

Calingaert, D.2010. Authoritarianism vs. the Internet. *Policy Review*. April & May: 63-75.

Liang, B. & Lu, H. 2010. Internet development, censorship and cyber crimes in China. *Journal of Contemporary Criminal Justice*. 26(1): 103-120.

http://edition.cnn.com/2010/WORLD/asiapcf/01/31/china.censorship/index.html?iref=allsearch

http://en.wikipedia.org/wiki/Green_Dam_Youth_Escort

http://news.bbc.co.uk/2/hi/business/8118055.stm

http://topics.nytimes.com/topics/news/international/countriesandterritories/china/internet_censorship/index.html

http://www.bbc.co.uk/news/world-asia-pacific-13455819

http://www.editorsweblog.org/2012/03/23/overcoming-censorship-how-chinese-bloggers-are-outsmarting-the-great-firewall

http://www.bbc.com/news/technology-17476788

http://www.internetfreedom.org/files/Research/battle-for-freedom-in-chinese-cyberspace.pdf

http://www.nytimes.com/2009/12/18/world/asia/18china.html?_r=1&ref=internetcensorship

http://www.nytimes.com/2011/03/22/world/asia/22china.html?_r=1

http://www.techworld.com.au/article/377359/china_blocks_microblogs_jasmine_revolution

http://www.vpnhero.com/news/china-internet-censorship-getting-worst/

http://www.vpnhero.com/news/china-to-monitor-public-internet-users-in-beijing/

4. FINLAND

4.1 INTRODUCTION

According to an OpenNet Initiative report, Finland along with the other Nordic countries of Denmark, Norway, Sweden, and Iceland is feeling the effect of the European Union in dealing with issues of file sharing, holding of rights and Internet service providers (http://opennet.net/research/regions/nordic-countries). In 2009 it was reported that Finland will join NATO's cyber-defense efforts in the defense of data systems against hostile or malicious acts (http://www.infowar-monitor.net/2009/05/finland-to-join-cyber-defence-effort-of-nato/). At some stage the European Union even mentioned a plan to create a "single secure European cyberspace" based on the blocking of what it considered as "illicit content". This suggestion met with concern and criticism from civil liberties groups (http://www.betrifft.de/dw/article/0,,15046720,00.html). When fully reflecting on censorship trends in Finland, it would be necessary to also consider it against the trends and actions taken in the wider contexts of the European Union of which Finland forms part.

Internet censorship in Finland will be discussed under negative as well as positive trends. The discussion is based on mining a wide variety of Internet resources. There may be many more trends than noted here, as well as many more examples of each. Each trend needs to be studied in more detail.

4.2 NEGATIVE TRENDS

4.2.1 Trends in issues of Internet related privacy

At the time of data mining no references specific to Internet related privacy were noted, apart from an OpenNet Initiative report mentioning the impact of the European Union on all countries forming part of it. There is increasing concern and debate about issues such as digital rights and privacy. The right to privacy is also discussed more widely in different political contexts (http://opennet.net/research/regions/nordic-countries). This led to an antipiracy initiative, the International Property Rights Enforcement Directive (IPRED), which gives holders of intellectual right and copyright the freedom to check the identities of people suspected to share files. It even allows them to get court orders that can force Internet service providers to share personal information about their users if they are suspected of digital piracy (http://opennet.net/sites/opennet.net/files/ONI_NordicCountries_2010.pdf).

4.2.2 Ubiquitous society and control

Finland, similar to other European countries such as Denmark, Norway, Sweden and the Netherlands uses a system of voluntary Internet blocking-filtering. This is run against a list of blocked websites containing illegal child pornography (http://www.kildarestreet.com/sendebates/?id=2010-04-22.179.0).

4.2.3 Trends in Internet related media being censored

Although Finland claims to focus on the censorship of child pornography, the blocking of other material has also been noted such as an English and Thai discussion of gay rights (http://www.effi.org/blog/kai-2008-02-18.html#what-is-censored), and a website with criticism on censorship.
It seems as if there is a strong focus on images of child pornography (http://libertus.net/censor/isp-blocking/ispfiltering-gl.html).

4.2.4 Trends in filtering and blocking Internet content and blocking software

The Finnish government started attempts at Internet censorship in 2006. Finnish Internet service providers (ISPs) were provided with a secret blocking list also referred to as a filtering list maintained by the Finnish police. According to some reports it is maintained by the National Bureau of Investigation (NBI). Although the list was intended to focus on child pornography or websites allegedly containing child pornography, especially websites outside Finland, it, in the end also includes websites that criticise pornography. In February 2008, the Electronic Frontier Finland (EFF) published an analysis of ''Finnish Internet censorship.'' According to their report, the filtering list contained about 1,700 websites, including a number of non-pornographic websites (http://opennet.net/sites/opennet.net/files/ONI_NordicCountries_2010.pdf).

A problem with the filtering list is that it seems as if there is no accountability expected from those maintaining the list, and that it has been noted to include a wider variety of websites than child pornography. The website, lapsiporno.info *[translates to childpornography.info]* is maintained by a Finnish Internet activist Matti Nikki. The website does not contain child pornography, but focuses on articles that criticise censorship. It also includes a list of blocked IP addresses. In 2008 it was reported that Electronic Frontier Finland (Effi) demanded from the National Bureau of Investigation (NBI) of Finland to explain why Finland's official censorship list also blocked this website for criticising Internet censorship. They noted: "Nikki has been one of the most vocal critics of the government's net censorship project" (http://www.effi.org/blog/kai-2008-02-18.html).

Most of the Finnish Internet service providers use the official secret censorship list of websites to be blocked in a Domain Name System (DNS) based filtering system. They are doing this under pressure from the government *(*http://www.effi.org/julkaisut/tiedotteet/lehdistotiedote-2008-02-12-en.html;

http://www.dbcde.gov.au/online_safety_and_security/cybersafety_plan/internet_service_provider_isp_filtering). The police send the censorship list to the Internet service providers. According to an Electronic Frontier Finland report it seems as if it is only send to selected Internet service providers. The Internet service providers are by law required to keep the censorship list secret. It seems as if some of them use an intercepting proxy server to do the filtering (http://www.effi.org/blog/kai-2008-02-18.html#how-the-censorship-works). Suspicions have been expressed that the filters might be extended to filter other websites. This has been met with concern and criticism from many privacy and advocacy groups (http://opennet.net/sites/opennet.net/files/ONI_NordicCountries_2010.pdf).

4.2.5 Trends in technologies to monitor and identify citizens using the Internet to express their opinion and applying "freedom of speech"

At the time of data mining no specific reports on trends in technologies to monitor and identify citizens using the Internet to express their opinion and applying freedom of speech were noted.

4.2.6 Criminalization of legitimate expression (e.g. thoughts, ideas, arguments) on the Internet

At the time of data mining no specific reports on criminalization of legitimate expression were noted with regard to Finland.

4.2.7 Trends in acts, regulations and legislation regarding use of the Internet and trends in government models regarding Internet censorship

According to an Electronic Frontier Finland report, the "Constitution of Finland, section 12, guarantees the freedom of expression. Censorship is absolutely forbidden by the constitution, except that there may be restrictions relating to pictorial programmes that are necessary for the protection of children. The censorship is implemented pursuant to the act on preventive measures on distribution of child pornography…" (http://www.effi.org/blog/kai-2008-02-18.html#how-the-censorship-works). This legislation was passed in 2006. It also gives the National Bureau of Investigation the authority to maintain a secret block list of foreign websites that distribute child pornographic images. This list is provided to Internet service providers who are under voluntary requirement to filter such websites (http://libertus.net/censor/isp-blocking/ispfiltering-gl.html).

Finland also has laws against mocking God or religion (Criminal Act, Ch. 17, Sec. 10). So far no such content has been noted to be filtered (http://opennet.net/sites/opennet.net/files/ONI_NordicCountries_2010.pdf).

4.2.8 Trends in new forms of Internet censorship, e.g. Halaal Internet, implied censorship such as user rating

At the time of data mining no reports on trends in new forms of Internet censorship were noted with regard to Finland.

4.2.9 Trends in support of Internet censorship, e.g. computer and Internet companies, search engines, Internet service providers

A report on an incident where a Finnish Internet service provider, Elisa, was ordered to block access to a Finnish Electronic Frontier Finland website was reported. This was part of action requested against The Pirate Bay to block access to a bunch of "pirate" websites. The website, piraattilahti.fi, was an advocacy website, which led to a comment on how "blocking over copyright" can very easily turn into "blocking over speech." (http://www.techdirt.com/blog/?tag=finland). Although Elisa refused to block the website, describing the blocking demands as “unreasonable”, the Helsinki District Court insisted on the blocking (http://cyberlaw.org.uk/2011/11/05/finnish-isp-ordered-to-block-the-pirate-bay/).

In another incident a Finnish court ordered an Internet service provider to prevent users accused of file sharing to use the Internet, without giving them any notice (http://www.techdirt.com/blog/?tag=finland).

4.2.10 Trends in enforcing regulations and Internet censorship

In Finland legal action is used to prevent the distribution of child pornography. Since 2005, Finland has maintained a voluntary program to restrict access to child pornography websites. There is, however, no obligation for Internet service providers to block websites on the secret list of censorship websites (http://www.scribd.com/doc/24138351/Untangling-the-Net-The-Scope-of-Content-Caught-by-Mandatory-Internet-Filtering).

4.2.11 Trends in Internet related communication surveillance

As a response to a terrorist incident in Norway in 2011, Finland decided to increase Internet surveillance to pick-up "weak signals" that could perhaps point to terrorist threats, and help to prevent somebody from copying and repeating the attacks in Norway. Finland is considering a variety of measures amongst other things to analyse what groups are saying (http://opennet.net/blog/2011/08/europe-responds-norway-attacks-calls-internet-monitoring-emerge; (http://www.techdirt.com/articles/20110726/19190515273/finnish-police-respond-to-norwegian-tragedy-increasing-internet-surveillance.shtml). These plans are in alliance with a pledge by the European counter-terrorism forces to increase Internet surveillance and the monitoring of cybercrimes.

4.3 POSITIVE TRENDS

4.3.1 Trends in reactions to Internet censorship

Electronic Frontier Finland (Effi) was founded in 2001 to defend active users and citizens of the Finnish society in the use of electronic resources such as the Internet, including the protection of digital rights. It is a founding member of the European Digital Rights (EDRi). It has been responsible for attempting to influence legislative proposals for example with regard to personal privacy, freedom of speech and user rights in copyright law. Their activities include making statements and press releases and participating actively in actual public policy and legal discussion. Electronic Frontier Finland also work closely with organisations elsewhere in Europe, the United States, etc. that shares its goals. Many members are also active researchers on issues concerning their mandate (http://www.effi.org/; http://www.effi.org/julkaisut/tiedotteet/lehdistotiedote-2008-02-12-en.html).

4.3.2 Attempts and means to side-step Internet censorship

From a blog maintained by Electronic Frontier Finland it is noted that it can be easy to side-step Internet censorship, even for people with minimal technical skills. All that is required is to use another domain name server than that of the Internet service provider responsible for the blocking; for example using OpenDNS, or a third party web proxy server (http://www.effi.org/blog/kai-2008-02-18.html#how-the-censorship-works).

4.3.3 Trends in cyber actions against Internet censorship

It appears that there is an increase in debate and conflict on Finnish blogs and other media about Internet censorship (http://libertus.net/censor/isp-blocking/ispfiltering-gl.html). The Electronic Frontier Finland has also demanded an explanation for adding a website that criticizes Internet censorship to the secret list of websites to be blocked (http://libertus.net/censor/isp-blocking/ispfiltering-gl.html).

4.3.4 Trends in innovative ways of showing opposition to Internet censorship

Finland has become the first country in the world to make Internet access a legal right. It is argued that every Finn should have access to a 1 Megabyte per second broadband Internet connection at home. This is considered a national right (http://www.cicsworld.org/blogs/tfprice/2010/04/post_1.html). There are also plans to increase this to 100 megabytes per second in 2015.

4.4 CONCLUSION

There is a concern about Internet censorship in Finland due to the secrecy of the list of censored websites. This is in view of the fact that there seems to be not much evidence of accountability for the selection of websites to be blocked, as well as the fact that there is evidence that more than child pornography is blocked. Moreover, there is also some concern for the impact of the European Union on Internet censorship in Finland. Even so, it seems as if reports on enforcing such censorship are not specked for concern about human rights and actions against individuals such as imprisonment.

4.5 REFERENCES

http://cyberlaw.org.uk/2011/11/05/finnish-isp-ordered-to-block-the-pirate-bay/

http://libertus.net/censor/isp-blocking/ispfiltering-gl.html

http://opennet.net/blog/2011/08/europe-responds-norway-attacks-calls-internet-monitoring-emerge

http://opennet.net/research/regions/nordic-countries

http://opennet.net/sites/opennet.net/files/ONI_NordicCountries_2010.pdf

http://www.betrifft.de/dw/article/0,,15046720,00.html

http://www.cicsworld.org/blogs/tfprice/2010/04/post_1.html

http://www.dbcde.gov.au/online_safety_and_security/cybersafety_plan/internet_service_provider_isp_filtering

http://www.effi.org/

http://www.effi.org/blog/kai-2008-02-18.html

http://www.effi.org/blog/kai-2008-02-18.html#how-the-censorship

http://www.effi.org/julkaisut/tiedotteet/lehdistotiedote-2008-02-12-en.html;

http://www.infowar-monitor.net/2009/05/finland-to-join-cyber-defence-effort-of-nato/

http://www.kildarestreet.com/sendebates/?id=2010-04-22.179.0works

http://www.scribd.com/doc/24138351/Untangling-the-Net-The-Scope-of-Content-Caught-by-Mandatory-Internet-Filtering

http://www.techdirt.com/articles/20110726/19190515273/finnish-police-respond-to-norwegian-tragedy-increasing-internet-surveillance.shtml

http://www.techdirt.com/blog/?tag=finland

5. LIBYA

5.1 INTRODUCTION

Limited Internet access and skills in using technology such as the Internet can sometimes be interpreted as implied censorship. In this regard Internet penetration in Libya is reported as very low; statistics reported in 2011 showed 354,000 people with access to the Internet. This equates to less than 6% of the population (http://communicationcrisis.net/2011/05/31/the-sound-of-silence-censorship-of-the-internet/).

Reports on Internet censorship in Libya are more limited when compared to countries such as Australia, Myanmar and China. In fact in 2006 Reporters Without Borders removed Libya from their list of "Enemies of the Internet" after a fact-finding visit found no evidence of Internet censorship. This was, however contradicted by the 2007-2008 OpenNet Initiative (ONI) technical test results. By August 2009, reports by the OpenNet Initiative on Internet censorship in Libya seemed to reflect selective censorship regarding politics, with no evidence regarding social, conflict/security, and Internet tools. This is somewhat in contrast with a remark found on the Internet that if the Reporters Without Borders list were made current, Libya would undoubtedly rank as one of the worst Internet censors in history (http://www.oafrica.com/ict-policy/internet-censorship-lessened/).

Reports on censorship in Libya seem to be strongly linked to its government and political climate. The overthrow of the Muammar Gaddafi government ended an era of mostly political censorship such as news blackouts by cutting access to the Internet, and a focus on a few political opposition websites – to slacking Internet censorship to such an extent, that the 2012 Reporters Without Borders report removed Libya from its list of countries under surveillance (http://en.wikipedia.org/wiki/Internet_censorship_by_country#.C2.A0Libya).

Internet censorship in Libya will be discussed under negative as well as positive trends. The discussion is based on mining a wide variety of Internet resources. There may be many more trends than noted here, as well as many more examples of each.

5.2 NEGATIVE TRENDS

5.2.1 Trends in issues of Internet related privacy

Not much on Internet related privacy was picked up through data mining. A report picked up during data mining noted some incidents of obtaining secret recordings of Muammar Gaddafi made during the Libyan revolution (http://www.ionglobaltrends.com/2012/05/libya-exclusive-wire-taps-on-gaddafis.html). When Libyan rebels took over the Government Headquarters in 2011 it became clear how Gaddafi, used technology to spy on his people e.g. by means of email infiltration (http://thenextweb.com/me/2011/08/30/how-far-gadhafi-went-to-monitor-libyas-internet-activity/).

5.2.2 Ubiquitous society and control

Although much of the reports on the control of the media concerns Libya's state-owned television (http://en.wikipedia.org/wiki/Free_speech_in_the_media_during_the_Libyan_civil_war#Television), there are also reports on online control. A number of Libyan online publications reported a wave of hacking incidents that targeted mostly independent and opposition websites; the people behind the attacks were not identified (http://opennet.net/research/profiles/libya).

In 2006 the OpenNet Initiative described Libya's Internet filtering programme as largely political in terms of content and suggested that the level of filtering and the types of websites being filtered were substantial. A follow-up study and subsequent report in 2009 showed that, while the type of content filtered was still the same, substantially less filtering was taking place. They thought this was due to efforts on the part of the government to move towards more openness.

It seems as if help on software to listen in on Yahoo chat or Skype may have been received from companies in the United Kingdom, Germany, France, the United States and other countries in the West (http://oraclesyndicate.twoday.net/STORIES/internet-spy-room-found-in-tripoli-packed-with-western-technology/comment).

Many Libyan opposition websites reported on the harassments of users of cyber cafés, especially at the time of the incidents in Benghazi in early 2012. According to the Libya Front website, the security forces at the time launched sudden and unusual visits to Internet cafés all over the country to check if the cafés owners register users' names. It seemed that most Internet café owners provided the Security Agency with the names of users, on a regular basis (http://old.openarab.net/en/node/362). Internet cafés had to register the names of their users and they had to expel those who visited prohibited websites (e.g. opposition and human rights websites). Café owners were furthermore required to get a license, and put up cautioning posters that could be seen everywhere on personal computers (PCs), as well as the internal and external walls of Libyan Internet cafés to warn users against visiting pornography websites and opposition websites (http://old.openarab.net/en/node/362).

5.2.3 Trends in Internet related media being censored

With recent unrest the media and especially foreign media were strongly blamed for the unrests in Libya. Internet television channels such as Libya Alhurra TV (Arabic: الحرة ل ي ب يا ق ناة) (meaning *Free Libya TV*), had to find alternative means to distribute information. They e.g. bypassed government blocks on the Internet in order to broadcast live images from Benghazi across the world (http://en.wikipedia.org/wiki/Free_speech_in_the_media_during_the_Libyan_civil_war#Television). Gaddafi's opinion of foreign television stations is reflected in his words referring to them as "stray dogs"; at the time the Libyan foreign minister also declared that journalists who enter Libya "illegally" would be treated by the pro-Gaddafi forces as agents working for Al-Qaeda (http://en.rsf.org/middle-east-north-africa-forced-being-used-to-restrict-01-03-2011,39655.html).

Recent (2012) unrests in Libya were marked by wide scale restrictions of freedom of expression. Furthermore, incidents were reported of acts of intimidation and restriction of information such as detention by the Internal Security Agency of members of the Libyan media (including writer/blogger Mohamed Ashim, director Taqi al-Din al-Shalawi, and editor-in-chief Abdel Fattah Bourwaq). Such acts also included forbidding local television stations from offering Al Jazeera, and blocking its website, as well as blocking social media websites such as Twitter and Facebook. Restrictions on the flow of information internally and externally were ensured by cutting Internet services across the country (http://cjfe.org/resources/protest_letters/restriction-and-intimidation-journalists-libya).

5.2.4 Trends in filtering and blocking Internet content and blocking software

In 2007 it was reported that Libya continues to block Internet content related to political opposition, content critical of the government, and websites that advocate the rights of the minority group Amazigh (Berbers). This persisted despite a claim toward greater openness and increasing freedom of the press (http://opennet.net/studies/libya2007).

With the rising threat from the Internet to government control over political information, the Libyan government appointed one of Gaddafi's closest friends to monitor and limit the growth of oppositional websites. Experts from Russia, Poland, and Pakistan were also summoned to Libya to help handle the situation. One tactic that emerged was to force owners of Internet cafés to place stickers on computers that warn visitors from logging onto websites considered as belonging to the opposition (http://opennet.net/studies/libya2007).

Beyond merely political content, the Libyan official ".ly" registry rules mandate that ".ly" domains "must not contain obscene, scandalous, indecent, or contrary to Libyan law or Islamic morality words, phrases or abbreviations." In 2007 the OpenNet Initiative ran tests on Libya's three Internet service providers at the time, namely Libya Telecom and Technology (LTT), Modern World of Communications (MWC), and Al-Falak. All three Internet service providers were found to block oppositional content such as the website of the Libyan Muslim Brotherhood (http://www.almukhtar.org) and the Libyan Constitutional Union (http://www.lcu-libya.co.uk; http://www.libyanconstitutionalunion.net). The three Internet service providers also blocked websites containing information critical of the Libyan government e.g. Libya for Ever (http://www.libya4ever.com), Libya al-Mostakbal (http://www.libya-almostakbal.com), and Libya Our Home (http://www.libya-watanona.com) (http://opennet.net/studies/libya2007). More recently (e.g. 2009) it seemed as if Internet filtering in Libya has become more selective, focusing on a few political opposition websites. This more lenient filtering policy coincides with what might be a trend towards more openness and increasing freedom of the press. However, the legal and political climate continues to encourage self-censorship in online media (http://opennet.net/research/profiles/libya).

In 2008-2009 tests indicated that some previously blocked websites were accessible from Libya while some opposition websites remained blocked. Websites that were blocked include the websites of the National Front for the Salvation of Libya (http://www.libyanfsl.com), Libya al-Mostakbal (http://www.libya-al-mostakbal.org), and Libya Watanona (http://www.libya-watanona.com) (http://opennet.net/research/profiles/libya). In 2011, Al Jazeera, whose coverage of political unrest in the Middle East and North Africa is widely watched in the Arab world, reported the jamming on its website where it offered alternative frequencies on the Arabsat, Nilesat and Hot Bird satellites (http://uk.reuters.com/article/2011/02/19/oukin-uk-jazeera-jamming-idUKTRE71I01920110219; http://www.goldsteinreport.com/article.php?article=13756). The blocking of the London based Libya Al-Youm [Libya Today] newspaper (http://www.libya-alyoum.com) was also reported in addition to sabotage by unidentified hackers which led to the destruction of all their files and content. This sabotage was associated with the newspaper's continued extensive coverage, despite the media black-out by the Libyan government (http://old.openarab.net/en/node/362).

Reported attempts to prevent access to the Internet under the Gaddafi government include Internet "curfews" of a few hours and blackouts cutting off access for up to four days (http://ucsdnews.ucsd.edu/pressreleases/internet_censorship_revealed_through_the_haze_of_malware_pollution/; http://www.arabipcentre.com/the-internet-in-libya.php; http://www.securitynewsdaily.com/480-internet-goes-dark-in-libya.html)
Cut offs especially marked the period of unrest against the dictatorship in 2011 (http://cpj.org/internet/2011/02/libyas-disordered-internet.php; http://leaksource.wordpress.com/2011/02/19/bahrain-libya-censoring-internet-to-silence-revolutions/).

5.2.5 Trends in technologies to monitor and identify citizens using the Internet to express their opinion and applying "freedom of speech"

Internet users in Libya told the Arabic media that security personnel and Internet café operators closely monitor Internet cafés and often harass Internet users. Several Internet cafés have been shut down by security, which has prompted café operators to do the monitoring themselves to avoid being shut down. Internet users also reported that notes are posted in Internet cafés warning users against accessing opposition websites (http://opennet.net/research/profiles/libya).

5.2.6 Criminalization of legitimate expression (e.g. thoughts, ideas, arguments) on the Internet

Libya has been marked by the fact that there is no independent broadcast or print media. Even Gaddafi's son, Seif, complained in 2006 that "in all frankness and transparency, there is no freedom of the press in Libya; actually there is no press, even, and there is no real 'direct people's democracy' on the ground" (http://communicationcrisis.net/2011/05/31/the-sound-of-silence-censorship-of-the-internet/).

Numerous incidents have been reported on members of the local media being detained by the Internal Security Agency as they attempt to report on the anti-government demonstrations and disseminate information to the public (http://www.cjfe.org/content/restrictions-and-intimidation-journalists-libya). On 12 August 2011 the Gaddafi regime e.g. announced that "any citizen in possession of a Thuraya [satellite telephone] must hold an authorisation to use it in accordance with the laws and regulations" and if not would "be punished according to the law that criminalizes communicating with the enemy in time of war, and stipulates penalties up to the death penalty" (http://en.wikipedia.org/wiki/Free_speech_in_the_media_during_the_Libyan_civil_war#Internet).

At the time when the Libyan opposition increasingly used the Internet to spread its message, the government also took strong action against journalistic freedom regarding the Internet. A famous Internet related case include a fifty-one-year-old bookseller, Abdel Razak Al Mansouri, who was arrested in January 2005 and interrogated about a number of his posts on the Akbar Libya website (http://www.akhbar-libya.com) in which he critised the government. Although he was never charged with a crime related to these Internet postings, he was charged, convicted, and sentenced to a year and a half in prison for possession of a gun without a license. After serving a year he was granted amnesty (http://opennet.net/studies/libya2007Cyberdissident Abdel Razak al Mansuri; http://en.rsf.org/libya-internet-writer-al-mansouri-gets-07-11-2005,15531.html).

Libya has also been reported as the first country to allegedly assassinate a writer because of his writings on the Internet. The journalist Deif Al-Ghazali resigned from Al-Zahf Al-Akhdar Newspaper, a state-owned publication, on 26 March 2005 because of his concerns with corruption. He started writing for Libyajeel.com about corruption and calling for reform. On 21 May 2006 he was kidnapped (according to unconfirmed sources he was kidnapped by internal security). Ten days after his kidnapping his body was found with all his limbs, including his fingers severed (http://old.openarab.net/en/node/362).

5.2.7 Trends in acts, regulations and legislation regarding use of the Internet and trends in government models regarding Internet censorship

According to reports the general situation regarding the law and the judicial system in Libya is very difficult to understand since the former ruler Gaddafi's "revolutionary legitimacy" gave him the right to regard his own personal ideas as constitutional reference which can replace both the Constitution and the Constitutional Court. In this unique context, any legal situation can always be subject to change. The legal situation in Libya was further complicated by the fact that there was/are no clearly assigned responsibilities for the authorities who were responsible for supervising and controlling the Internet (http://old.openarab.net/en/node/362).

In spite of the absence of any legal framework that identifies the mechanisms for censoring and blocking websites, the Libyan authorities have been reported to impose censorship on opposition websites. In some cases, the websites were even completely destroyed. All Libyan opposition websites that come to the attention of the authorities were blocked. If someone tried to view these pages in an Internet café, they were expelled and could be reported to the security services which at some stage even imported Russian Internet experts to tighten the government’s control on the use of the Internet (http://old.openarab.net/en/node/362).

The state-owned General Post and Telecommunications Company (GPTC), run by Gaddafi’s son, Mohamed al-Gaddafi, regulated and operated Libya’s telecommunications infrastructure, providing “international and local voice services, digital leased lines, telex, fax, mobile (through a partially owned subsidiary) and Internet services.” The GPTC also owned the country’s primary Internet service provider, Libya Telecom and Technology (LTT), which offers Internet services via dialup, DSL, broadband, and satellite. Competing companies were subordinated to Libya Telecom and Technology which seemed to maintain a monopoly at the time of an OpenNet Initiative report appearing in 2007 (It was not checked if this is still the case.) (http://opennet.net/studies/libya2007).

5.2.8 Trends in new forms of Internet censorship, e.g. Halaal Internet, and implied censorship such as user rating

At the time of data mining, nothing was noted on new forms of Internet censorship.

5.2.9 Trends in support of Internet censorship, e.g. computer and Internet companies, search engines, Internet service providers

At the time of data mining trends in support of Internet censorship were not noted.

5.2.10 Trends in enforcing regulations and Internet censorship

In 2006 Libya's media was reported to be the most tightly controlled in the Arab world. The government owned and controlled all print and broadcast media which was expected to reflect state policies and not to allow news or views critical of Gaddafi or the government. Although satellite television and the Internet were available at the time, the government blocked undesirable political websites. Although the Internet was used by independent writers and journalists to share their views, they were taking very high risks. Dayf al-Ghazal al-Shuhaibi, who wrote for a London-based opposition website, was e.g. found shot in the head in Benghazi. The fact that no one was charged with the murder, seemed like a message to would-be critics (http://cpj.org/reports/2006/05/10-most-censored-countries.php).

5.2.11 Trends in Internet related communication surveillance

When Libyan rebels took over the Government Headquarters in 2011 it became clear how Gaddafi, used technology to spy on his people e.g. by means of email infiltration. Libyan officials are known to have met with various international companies to implement a filtering and monitoring system that ran deep through Libya’s Internet system. Boeing Co.’s Narus is reportedly one of those companies, but the company denied such involvement. Amesys, a French company, seems to have installed ‘deep packet inspection‘ technology for the Libyan government in 2009, giving them data mining, eavesdropping and censorship capabilities (http://thenextweb.com/me/2011/08/30/how-far-gadhafi-went-to-monitor-libyas-internet-activity/). This included the ability to record, store, analyze and display information in real time information, and to monitor a wide range of protocols, including mail, voice over Internet Protocol (VoIP), webmail, chat, web browsing. Services like Hotmail, Yahoo Mail and Gmail, as well as MSN, Yahoo, AIM chat, and peer-to-peer (P2P) file sharing could also be monitored at the time. It is suspected that the Chinese telecom company ZTE Corp might also have aided Libya as well as VASTech SA, a South African firm (http://thenextweb.com/me/2011/08/30/how-far-gadhafi-went-to-monitor-libyas-internet-activity/). Libya looked for advanced tools to control Skype, to censor YouTube videos and to block Libyans from disguising their online activities by using "proxy" servers (http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html). August 30, 2011, a 22-year-old student who helped organise some of the biggest protests near Tripoli said in a Skype chat with a foreign journalist before fleeing to Egypt: "We're likely to disappear if you aren't careful". On March 1, two of his friends were arrested four hours after calling a foreign correspondent from a

Tripoli-based cellphone. Reports of harassing bloggers, smearing their reputation, and invading their privacy and emails were also noted (http://www.wired.com/threatlevel/2012/05/ff_libya/). Morayef describes Libya’s Internet monitoring as both sophisticated and rudimentary (http://thenextweb.com/me/2011/08/30/how-far-gadhafi-went-to-monitor-libyas-internet-activity).

5.3 POSITIVE TRENDS

5.3.1 Trends in reactions to Internet censorship: changes in groups, group dynamics, responses and actions of groups

At the time of data mining, nothing was noted on changes on reactions to Internet censorship.

5.3.2 Attempts and means to side-step Internet censorship (e.g. specialised software such as FREEBIRD, tracing blackouts, attempts to involve the pubic and public opinion)

When Libya faced an Internet crack-down similar to the one faced in Egypt, French Data Network, offered free dial-up Internet for Libyans. Even when the Internet was off at the time, Libyans could use landlines and faxes to disseminate information in the country (http://www.readwriteweb.com/cloud/2011/02/using-fax-machines-to-route-ar.php).

5.3.3 Trends in cyber actions against Internet censorship, e.g. cyber and virtual demonstrations and protest

At the time of data mining, nothing was noted on trends in cyber actions against Internet censorship.

5.3.4 Trends in innovative ways of showing opposition to Internet censorship

The government’s means to disrupt the Internet was studied by a team of scientists led by the Cooperative Association for Internet Data Analysis (CAIDA) at the University of California, San Diego. Their study focused on the use of malware where malicious software or network activity generate unsolicited traffic in attempting to compromise or infect vulnerable machines. Such traffic “pollution” is commonly referred to as Internet background radiation (IBR) and is ubiquitously observable on most publicly accessible Internet links (http://ucsdnews.ucsd.edu/pressreleases/internet_censorship_revealed_through_the_haze_of_malware_pollution/).

In-spite of a change in government in Lybia, the general public still haven't had much access to the Internet, and services are often not available. At times when the Internet was disconnected in

2011, people turned to satellite phones or international dial-up, considered to be dangerous, slow, expensive ways to get news out (http://www.renesys.com/blog/2011/08/the-battle-for-tripolis-intern.shtml).

5.4 CONCLUSION

Based on the data mined it is difficult to take a stance on Internet censorship in Libya: on the one hand it is no longer on the Reporters Without Borders list as an "Enemy of the Internet", on the other hand based on some of the reports, it seems as if under the Gaddafi rule there were serious reports of communication surveillance and censorship. In addition, to limitations on Internet access, there is restricted media freedom. The nature of control since the 2011 uprisings is not quite clear, although there is suspicion that it is still very much politically focused.

5. 5 REFERENCES

http://cjfe.org/resources/protest_letters/restriction-and-intimidation-journalists-libya
http://cpj.org/internet/2011/02/libyas-disordered-internet.php
http://cpj.org/reports/2006/05/10-most-censored-countries.php
http://communicationcrisis.net/2011/05/31/the-sound-of-silence-censorship-of-the-internet/
http://en.rsf.org/middle-east-north-africa-forced-being-used-to-restrict-01-03-2011,39655.html
http://en.rsf.org/libya-opposition-journalist-daif-al-06-06-2005,14012.html
http://en.rsf.org/libya-cyberdissident-abdel-razak-al-07-03-2006,16156.html
http://en.rsf.org/libya-internet-writer-al-mansouri-gets-07-11-2005,15531.html
http://en.rsf.org/libya-international-satellite-broadcasts-07-12-2005,15855.html
http://en.rsf.org/libya-seif-gaddafi-asked-to-intercede-on-22-08-2005,14748.html
http://en.wikipedia.org/wiki/Free_speech_in_the_media_during_the_Libyan_civil_war#Internet
http://en.wikipedia.org/wiki/Free_speech_in_the_media_during_the_Libyan_civil_war#Television
http://en.wikipedia.org/wiki/Internet_censorship_by_country#.C2.A0Libya
http://leaksource.wordpress.com/2011/02/19/bahrain-libya-censoring-internet-to-silence-revolutions/
http://old.openarab.net/en/node/362
http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html
http://oraclesyndicate.twoday.net/STORIES/internet-spy-room-found-in-tripoli-packed-with-western-technology/comment
http://opennet.net/research/profiles/libya)
http://opennet.net/studies/libya2007
http://thenextweb.com/me/2011/08/30/how-far-gadhafi-went-to-monitor-libyas-internet-activity/
http://ucsdnews.ucsd.edu/pressreleases/internet_censorship_revealed_through_the_haze_of_malware_pollution/

http://www.aljazeera.com/indepth/spotlight/libyaontheline/2012/05/201251173614897923.html

http://www.arabipcentre.com/the-internet-in-libya.php

http://www.cjfe.org/content/restrictions-and-intimidation-journalists-libya

http://www.goldsteinreport.com/article.php?article=13756

http://www.ionglobaltrends.com/2012/05/libya-exclusive-wire-taps-on-gaddafis.html

http://www.oafrica.com/ict-policy/internet-censorship-lessened/

http://www.securitynewsdaily.com/480-internet-goes-dark-in-libya.html

http://www.readwriteweb.com/cloud/2011/02/using-fax-machines-to-route-ar.php

http://www.renesys.com/blog/2011/08/the-battle-for-tripolis-intern.shtml

http://www.wired.com/threatlevel/2012/05/ff_libya/

6. MYANMAR

6.1 INTRODUCTION

Myanmar (or Union of Myanmar) also known as Burma (or Union of Burma) by bodies and states which do not recognise the ruling junta, is one of Asia's poorest countries. It is a country associated with scant respect for fundamental human rights, and some of the most stringent government attempts at censorship and control. Over several decades Myanmar has been marked by military dictatorship and what is often referred to as draconian rule. Widespread and systematic violations of human rights have frequently been reported. This includes restrictions on freedom of expression, especially in election events and periods leading up to elections. Reporters Without Borders lists Myanmar as an "Enemy of the Internet", and has described its legislation as "one of the most liberticidal laws in the world"; being listed 174th out of 178 counties in the 2010 Reporters Without Borders press freedom report (http://en.rsf.org/burma-burma-12-03-2012,42076.html; http://en.rsf.org/burma-additional-10-year-jail-term-08-02-2011,39498.html).

Apart from pervasive censorship, Myanmar is marked by very low Internet penetration, a lack of knowledge and skills in using the Internet, very high costs in using the Internet and very slow bandwidth, which in itself are all forms of indirect censorship. In 2010 Internet penetration was estimated at 0.2%, and later in 2012 at 1% (http://www.guardian.co.uk/technology/2010/oct/21/internet-web-censorship-asia?INTCMP=SRCH; http://en.rsf.org/burma-burma-12-03-2012,42076.html).

Internet censorship in Myanmar will be discussed under negative as well as positive trends. The discussion is based on mining a wide variety of Internet resources. There may be many more trends than noted here, as well as many more examples of each.

6.2 NEGATIVE TRENDS

In general there seems to be a tightening of government control contrary to statements from the new government that it intends to lighten control and ease censorship e.g. by Ye Htut, director general of Mynamar's Ministry of Defense. Although a sneak preview of Myanmar's opposition leader, Aung San Suu Kyi's, in an upcoming election, has been leaked in 2011 as a video on the Internet, part of her speech was still reported to be censored (http://www.google.com/hostednews/ap/article/ALeqM5jtazLG6s6e9aT4oNt-HMZhqUlRnw?docId=315b99ed60de469584a2844a17f79b2d).

6.2.1 Trends in issues of Internet related privacy

It seems as if the use of all .mm websites (with Myanmar as country domain) and email addresses are especially closely monitored by the ruling military junta, and that there is an increase in blocking the use of email (http://www.guardian.co.uk/technology/2010/oct/21/internet-web-censorship-asia?INTCMP=SRCH). Emails are also frequently checked e.g. at cybercáfes and at some stages even at hotels (http://www.guardian.co.uk/technology/2003/jul/22/burma.onlinesupplement?INTCMP=SRCH).

6.2.2 Ubiquitous society and control

Service records of all users of Public Access Centres (PACs) including the date, time, screen shot, and URLs must be submitted once a month to the Directorate of Communication. The leasing or transferring of a PAC license is prohibited (http://en.rsf.org/burma-surveillance-of-media-and-internet-17-05-2011,40296.html). Cyber cafés are by law required to do very close monitoring (http://opennet.net/studies/burma) and the Press Scrutiny and Registration Division (PSRD) and Burma's Censorship Office also take on active roles in censorship (http://www.news24.com/SciTech/News/Myanmar-blogger-pushes-peoples-voice-20120229).

In 2003 it was reported that even business centres at five-star hotels did not provide Internet access: guests could only send and receive email through hotel accounts where staff printed the emails and handed guests a printed copy (http://www.guardian.co.uk/technology/2003/jul/22/burma.onlinesupplement?INTCMP=SRCH).

6.2.3 Trends in Internet related media being censored

Email is closely monitored, and the use of external hard drives, USB flash drives, CDs, and Internet telephony services (VoIP) to make international calls (e.g. Skype, Gtalk, Pfingo and VZO) have been banned (http://en.rsf.org/burma-burma-12-03-2012,42076.html). At times the sharing of video and image files is also prevented by limiting bandwidth e.g. during the November 2010 elections (http://en.wikipedia.org/wiki/Internet_in_Burma#Internet_shutdowns_and_reductions_in_bandwidth).

Blocking and banning of websites and blogs are frequently reported especially those of political opposition groups, organisations promoting democratisation and independent news websites. In addition, pornographic and gambling websites as well as those relating to human rights are subject to frequent blockage. Access to free email services such as Yahoo! Mail and Gmail as well as video-sharing through YouTube has been sporadically blocked. This also applies to Facebook, Google's Blogspot and Twitter as a microblogging site, and Global Voice (http://en.wikipedia.org/wiki/Internet_in_Burma; http://opennet.net/news/more-websites-banned-myanmar-global-voices-banned-too).

6.2.4 Trends in filtering and blocking Internet content and blocking software

The government's attempts to restrict Internet access include cutting down Internet services, slowing down services to a "snail's pace", disrupting the use of email services (e.g. 10 minutes after use), limiting access to selected local content, blocking access to websites, and forbidding access to websites (http://www.ifex.org/burma/2010/10/28/internet_connection/). The restrictions are so severe in terms of the limited number of websites to which there is access that reference is often made to "Myanmar Wide Web" instead of the World Wide Web. Even this has been reported to be monitored by official censors. In an interview granted to *Rolling Stone* magazine, American hacker and WikiLeaks member Jacob Applebaum exposed the scope of the censorship by showing that only 118 of the country's 12,284 IP addresses are not blocked by the regime and have access to the World Wide Web (http://en.rsf.org/burma-burma-11-03-2011,39754.html).

Recently the Internet infrastructures have also been adapted to enable the government to cut off the public's Web access without affecting official connections. This has been achieved through a reorganization of Internet service providers which will also allow the authorities to increase online surveillance and repression. Internet users will be allocated to three Internet service providers, instead of the two they had before. One will be reserved for the Myanmar defense ministry, one for the government and one for the public. Under this system, the government will be able to totally or partially block the population's access without affecting government or military connections. This will also allow the defense ministry to directly control Internet traffic at the point of entry into Burma (http://en.rsf.org/burma-burma-11-03-2011,39754.html).

In October 2010 a national portal called "Yadanabon Cyber City" was introduced that will supposedly offer an email service (Ymail) and a chat service (Ytalk) as alternatives to Gmail and Gtalk, and which will make it even easier for the authorities to monitor users' online communications. The portal is run by the Burmese junta-controlled Yatanarpon Teleport Company. Although the portal may offer the benefit of faster and improved Internet access, it may also make Internet surveillance and repression easier. The cost of the new service, which will be passed on to the public, may also curb any growth in the Internet penetration rate: the average salary of the people of Myanmar is 27 U.S. dollars per month and Internet cafés charge 54 cents per connection hour (http://en.rsf.org/burma-burma-11-03-2011,39754.html).

Myanmar is also frequently subjected to partial or total Internet shutdowns and cyber attacks aimed at slowing down access e.g. in the form of distributed denial of service (DDoS) which specifically affects exiled Burmese media websites such as Irrawaddy and the Democratic Voice of Burma (DVB) (http://en.rsf.org/burma-burma-11-03-2011,39754.html).

6.2.5 Trends in technologies to monitor and identify citizens using the Internet to express their opinion and applying "freedom of speech"

Recently (2012) it has been reported that undetectable Internet "sniffers" will be placed on the server of the Internet service provider that will be reserved for the public. The intention is to retrieve diverse confidential data (http://en.rsf.org/burma-burma-12-03-2012,42076.html).

6.2.6 Criminalization of legitimate expression (e.g. thoughts, ideas, arguments) on the Internet

Myanmar is marked by the detention and harsh punishment of especially journalists and bloggers e.g. the journalist Hla Hla Win for uploading data to the Internet that was "damaging to the security of the military regime" as well as the blogger Nay Phone Latt. In the words of Nay Phone Latt, the prison sentences are very severe “To frighten the other bloggers and other IT-related youth, they sentenced me to so many years” (http://www.hrw.org/news/2012/01/06/burmas-prisons-should-not-be-limits-international-monitors; http://www.news24.com/SciTech/News/Myanmar-blogger-pushes-peoples-voice-20120229).

6.2.7 Trends in acts, regulations and legislation regarding use of the Internet and trends in government models regarding Internet censorship

The banning of Internet censorship circumvention methods such as bypass and proxy websites e.g. http://www.polysolve.com**, http://**www.glite.sayni.net**, http://**www.3proxy.com**, http://**www.unipeak.com has been reported over many years (http://citizenhacktivist.wordpress.com/2007/01/14/internet-censorship-in-burma-stepped-up/). Businesses offering access need to register as Public Access Centres and are required to keep logs. Network connections need to be registered, and the sharing of registered connections are punishable (*Access denied*… 2008:339-240).

There has been a strict control of cyber cafés for quite some time. The Law requires them to keep records of customers’ activities, to provide the police access to records on request, post signs on forbidden sites, install CCTV cameras and at least four security staff to monitor users. Cyber cafés operate under license from the Myanmar Information Communications Technology Development Corporation (MICTDC), where the licenses also require café owners to take screenshots of user activity every five minutes and deliver CDs containing these images (http://opennet.net/studies/burma). Cyber cafés are also subject to unexpected inspections. A decline in the use of cyber cafés has been noted (http://www.ifex.org/burma/2010/10/28/internet_connection/).

6.2.8 Trends in new forms of Internet censorship e.g. Halaal Internet, implied censorship such as user rating

The following are not really new forms of trends, but need to be noted. In Myanmar people are kept from accessing the Internet through high costs for connecting and for use, limited Internet service providers, and not addressing the vast majority of people lacking IT and Internet use skills. A 2012 report stated that just 1% of the population enjoys Internet access, and the country only has about 500 cyber cafés, mainly in large cities (http://en.rsf.org/burma-burma-12-03-2012,42076.html). Internet service providers increased from two to three – all government controlled (http://en.rsf.org/burma-burma-11-03-2011,39754.html).

6.2.9 Trends in support of Internet censorship

Fortinet, a California-based company, provides the government with software that limits the material that can be surfed (http://www.vpnhero.com/articles/buypass-internet-censorship-burma-myanmar/). Some Myanmar Internet service providers have been reported to acquire censorship equipment and hardware from the Chinese subsidiary of the Franco-American company Alcatel-Lucent (http://en.rsf.org/burma-burma-11-03-2011,39754.html).

6.2.10 Trends in enforcing regulations and Internet censorship

Restrictions are placed on content and opinions through the Electronic Act against people "giving talks and publishing and distributing publications with the intention of tarnishing the image of the State" (http://www.hrw.org/news/2010/07/01/universal-periodic-review-submission-myanmar-burma).
Other legislation regulating the use of the Internet includes the Computer Science Development Law (1996), the Wide Area Network Order (2002), and the Electronic Transactions Law (2004), while the Printers and Publishers Registration Act (1962) regulates the media. This applies especially during elections and periods leading up to elections.

6.2.11 Trends in Internet related communication surveillance

At the time of data mining, nothing specifically related to communication surveillance were noted.

6.3 POSITIVE TRENDS

On the surface it seems as if the Government is making an attempt to slacken the strict control, and as if there is more free circulation of information on the Internet. A few journalists and bloggers were released as part of a larger series of amnesties by the regime in the second half of 2011 (http://en.rsf.org/burma-burma-12-03-2012,42076.html). The first phase of the Yatanarpon cyber city which officially opened 14 December 2007 has been completed (http://www.digital-review.org/uploads/files/pdf/2009-2010/chap-32_myanmar.pdf). Although there are no independent daily newspapers, online news sites, however, seem to be growing (http://www.ft.com/cms/s/0/1a78c348-6e92-11e1-a82d-00144feab49a.html#axzz1pvL3EsBa).
Unblocking YouTube, BBC, Reuters, Thailand's Bangkok Post, Singapore's Straits Times, *Radio Free Asia*, *Irrawaddy*, *Democratic Voice of Burma* (DVB), and the Burmese version of *Voice of America* have also been reported (http://en.wikipedia.org/wiki/Internet_in_Burma; Global Voices Online).

6.3.1 Trends in reactions to Internet censorship: changes in groups, group dynamics, responses and actions of groups

At the time of data mining, nothing specifically relating to trends in reactions to Internet censorship was noted.

6.3.2 Attempts and means to side-step Internet censorship (e.g. specialised software such as FREEBIRD, tracing blackouts, attempts to involve the public and public opinion)

The use of Your-freedom.net and Yeehart.com, both of which similarly maintain new, updated versions to bypass government firewalls, has been reported. The same is true for various encrypted e-mail services, including the hyper-secure Hushmail.com, which many local and exile-based journalists use (http://atimes.com/atimes/Southeast_Asia/II21Ae01.html). A new software program (http://arxiv.org/pdf/1106.2696v1) aims to prevent the authorities tracking down photographers at demonstrations (http://www.guardian.co.uk/technology/2011/jul/03/keeping-snappers-out-of-picture?INTCMP=SRCH).

6.3.3 Trends in cyber actions against Internet censorship e.g. cyber and virtual demonstrations and protests

The number of bloggers has increased. In 2011 it was reported that there were 1,500 bloggers, 500 of whom blog regularly. When including Burmese bloggers based abroad, this number totals 3,000 (http://en.rsf.org/burma-burma-11-03-2011,39754.html).

6.3.4 Trends in innovative ways of showing opposition to Internet censorship

At the time of data mining, nothing specifically relating to trends in ways of showing opposition to Internet censorship was noted.

6.4 CONCLUSION

Although some positive trends were noted regarding Internet censorship in Myanmar, in view of the proclaimed intentions of the government, Myanmar still seems to be a country marked by severe Internet censorship, especially on political issues, and this is enforced by the government. Even if the legislation is slackened and more freedom of expression allowed, implied censorship would still manifest in a country with low Internet penetration, slow bandwidth, high costs of accessing the Internet, as well as the lack of skills in using the Internet among its people.

6.5 REFERENCES

http://atimes.com/atimes/Southeast_Asia/II21Ae01.html

http://arxiv.org/pdf/1106.2696v1

http://citizenhacktivist.wordpress.com/2007/01/14/internet-censorship-in-burma-stepped-up/

http://en.rsf.org/burma-additional-10-year-jail-term-08-02-2011,39498.html

http://en.rsf.org/burma-burma-12-03-2012,42076.html

http://en.rsf.org/burma-burma-11-03-2011,39754.html

http://en.rsf.org/burma-surveillance-of-media-and-internet-17-05-2011,40296.html

http://en.wikipedia.org/wiki/Internet_in_Burma#Internet_shutdowns_and_reductions_in_bandwidth)

http://en.wikipedia.org/wiki/Internet_in_Burma

http://opennet.net/studies/burma

http://opennet.net/news/more-websites-banned-myanmar-global-voices-banned-too

http://www.digital-review.org/uploads/files/pdf/2009-2010/chap-32_myanmar.pdf

http://www.ft.com/cms/s/0/1a78c348-6e92-11e1-a82d-00144feab49a.html#axzz1pvL3EsBa

http://www.google.com/hostednews/ap/article/ALeqM5jtazLG6s6e9aT4oNt-MZhqUlRnw?docId=315b99ed60de469584a2844a 17f79b2d)

http://www.guardian.co.uk/technology/2003/jul/22/burma.onlinesupplement?INTCMP=SRCH

http://www.guardian.co.uk/technology/2010/oct/21/internet-web-censorship-asia?INTCMP=SRCH

http://www.guardian.co.uk/technology/2011/jul/03/keeping-snappers-out-of-picture?INTCMP=SRCH

http://www.hrw.org/news/2012/01/06/burmas-prisons-should-not-be-limits-international-monitors

http://www.hrw.org/news/2010/07/01/universal-periodic-review-submission-myanmar-burma

http://www.ifex.org/burma/2010/10/28/internet_connection/

http://www.news24.com/SciTech/News/Myanmar-blogger-pushes-peoples-voice-20120229

http://www.vpnhero.com/articles/buypass-internet-censorship-burma-myanmar/

7 SINGAPORE

7.1 INTRODUCTION

Officially the Republic of Singapore claims to focus on promoting social values and maintaining national unity when filtering Internet content and blocking access. Officially the focus is on pornography and content encouraging ethnic or religious strife (http://opennet.net/studies/singapore). Taking a closer look at the incidents reported it seems, however, as if criticism against the government and thus freedom of speech is also under control. The purpose of Internet censorship in Singapore has been reported as "to promote and facilitate the growth of the Internet while at the same time safeguarding social values as well as racial and religious harmony" (http://opennet.net/research/profiles/singapore).

Internet censorship in Singapore will be discussed under negative as well as positive trends. The discussion is based on mining a wide variety of Internet resources. There may be many more trends than noted here, as well as many more examples of each. Each trend needs to be studied in more detail.

7.2 NEGATIVE TRENDS

7.2.1 Trends in issues of Internet related privacy

At the time of data mining no specific references to incidents related to Internet privacy were noted.

7.2.2 Ubiquitous society and control

Internet services in Singapore are provided by the three major Internet service providers (ISPs). They are regulated by the Media Development Authority (MDA) and are required to block a number of websites containing "objectional" material, especially pornographic material such as Playboy and YouPorn. These are described as "mass impact objectionable" material.

Flickr, the social networking site for photo's, have content filters, which users are expected to use on their photos. Users must choose a safety level (safe, moderate, or restricted) and a content type (photo, video, illustration, or screenshot) for their content. They can also set a SafeSearch preference in order to determine what they see when searching for content on Flickr. These settings are used to filter content for users in Singapore, Hong Kong, India, and South Korea, where users are only able to see photos deemed 'safe' by Flickr staff (http://opennet.net/policing-content-quasi-public-sphere).

Some websites in Singapore are blocked due to user trial and error/research e.g. certain YouTube uploads. An example of a banned website is Chick.com – a fundamentalist Christian tract website which was probably banned due to tracts of Islam-bashing, and the Singapore government's sensitivity to anti-Islam sentiments which are not accepted in their aim for social and religious harmony (http://en.wikipedia.org/wiki/Internet_censorship_in_Singapore).

A report was also noted on giving parents more control at home over their children's use of the Internet (http://opennet.net/news/singapore-censorship-review-panel-wants-give-parents-more-control-over-childrens-internet-tv-ex).

7.2.3 Trends in Internet related media being censored

According to the Media Development Authority (MDA) it blocks only a symbolic list of 100 websites (primarily pornography) as a symbol of the state's disapproval of such content. In addition, the Ministry of Education of Singapore blocks access to pornographic and similar websites on its proxy servers, and the three major Internet service providers each offers, optional, filtered Internet access that blocks additional websites for a minimal monthly fee (http://opennet.net/studies/singapore).

In the past there have been reports on banning a gay website for promoting promiscuous sexual behaviour and allegedly recruiting underage boys for sex and nude photography (http://en.wikipedia.org/wiki/Internet_censorship_in_Singapore). In a 2004-2005 report by OpenNet Initiative it was proclaimed that technical censorship by the government (i.e. the State) in Singapore is actually very limited with the focus mostly on pornography and illegal drugs. Often such content might, however, be found on other websites that are not blocked (http://opennet.net/studies/singapore; http://opennet.net/studies/singapore#toc2e).

Control of Internet material and content is set against the censorship guidelines drawn up by the Singapore government. In essence materials originating from homes are more strongly censored than material origination from businesses. Materials originating from younger people are more heavily censored, and artistic materials are less heavily censored. Also, if it is considered that materials are used by fewer people, censorship is less heavy. In practice these principles can lead to conflict (http://www.browsys.com/search/index.php?ref=self&side=top&q=censorship+and+the+internet%3A+a+singapore+perspective)

7.2.4 Trends in filtering and blocking Internet content and blocking software

The regulation of Internet content in Singapore does not depend much on technological methods to block access; it depends mostly on access controls and legal pressures to keep people from posting content that is considered “objectionable”. In comparison to other countries that implement mandatory filtering, Singapore's technical filtering system seems very limited, much more than for example in Australia (http://opennet.net/blog/2005/09/internet-filtering-singapore-2004-2005; http://www.efa.org.au/Campaigns/compareasia.html).

Internet service providers are required to block access to 100 high impact pornographic websites, identified by the Singapore Broadcasting Authority as objectionable as well as access to newsgroups which contain "prohibited" content. Adult verification mechanisms are not required for material unsuitable for children.

The National University of Singapore has been reported to have different servers for staff and students. The idea is for staff to be less heavily censored in terms of access to materials than students. Usenet news groups are censored using government guidelines e.g. Usenet groups accessed through the local PTT, Singapore Telecom, are more heavily censored than those accessed through the local universities (http://www.browsys.com/search/index.php?ref=self&side=top&q=censorship+and+the+internet%3A+a+singapore+perspective)

7.2.5 Trends in technologies to monitor and identify citizens using the Internet to express their opinion and applying “freedom of speech”

For both Internet content and service providers, there are penalties for non-compliance with restrictions on prohibited material. At the time of data mining it was only noted that Singapore does not show strong reliance on technology to monitor people’s use of the Internet.

7.2.6 Criminalization of legitimate expression

The government employs various means to control freedom of expression through the Internet. Incidents of government using lawsuits, fines, and criminal prosecution or threats of litigation against bloggers and Internet content providers regarding content “related to sensitive issues” were noted (http://opennet.net/research/profiles/singapore). These include a case against Sintercom in July 2001 where the founder, Dr Tan Chong Kee, shut down the website rather than register it under the *Broadcast Authority Act* (now Media Development Authority); he considered the act ambiguous. There was also the case of Chen Jiahao, a blogger, who in 2005 had to apologise and shut down his blog containing criticisms on the government agency A*STAR, after its Chairman Philip Yeo threatened to sue for defamation. In another incident in 2005 three people were arrested and charged under the Sedition Act for posting racist comments on the Internet; two were sentenced to imprisonment. Actions of suspension against students "flaming" on their blog were also reported, as well as bloggers being sentenced for posting racists material (http://en.wikipedia.org/wiki/Internet_censorship_in_Singapore; http://opennet.net/blog/2005/10/singapore-blocks-gay-web-site). More recently actions against government critics and human rights defenders for exercising their right to freedom of expression seem to continue. This includes reports of arbitrary detention, judicial caning and the death penalty (http://www.amnesty.org/en/library/asset/POL10/001/2011/en/519da037-1492-4620-9ed5-cac8f1cfd591/pol100012011en.pdf).

7.2.7 Trends in acts, regulations and legislation regarding use of the Internet and trends in government models regarding Internet censorship

It seems that Internet censorship in Singapore (described by the government as a “light-touch” regulatory framework) mostly depends on a combination of access controls (such as requiring political websites to register for a license) and legal pressures (such as defamation lawsuits and the threat of imprisonment). The intention is to prevent people from posting objectionable content (http://opennet.net/research/profiles/singapore). Since July 1996 regulation of content is done by the Singapore Broadcasting Authority (SBA). The Media Development Authority (MDA) regulates the Internet service providers. Both Internet content providers and Internet service providers require a license under the Class License Scheme. They need to comply with the Class Licence Conditions and the Internet Code of Practice. The latter includes a definition of "prohibited material". Prohibited content includes content which depicts nudity in a titillating fashion; promotes sexual violence; shows people engaged in explicit sexual activity; advocates homosexuality or lesbianism; shows sexual activity by a person who is or appears to be less than 16 years old; depicts incest, bestiality, pedophilia, or necrophilia; depicts extreme violence or cruelty; or "glorifies, incites or endorses ethnic, racial or religious hatred, strife or intolerance (http://opennet.net/studies/singapore#toc2e). The Class License Scheme is stipulated by the Broadcasting Act. It seems as if the Scheme does not apply to all Internet content providers (http://www.efa.org.au/Issues/Censor/cens3.html#sing).

Regulations and legislation in Singapore is aimed at promoting responsible use of the Internet, while giving people some flexibility (http://opennet.net/research/profiles/singapore). Other means of influencing Internet use are thus the promotion of self-regulation and public education.

7.2.8 Trends in new forms of Internet censorship, e.g. Halaal Internet, implied censorship such as user rating

At the time of data mining, no specific reports on new forms of Internet censorship were noted.

7.2.9 Trends in support of Internet censorship, e.g. computer and Internet companies, search engines, Internet service providers

At the time of data mining, no specific reports on trends in support of Internet censorship were noted.

7.2.10 Trends in enforcing regulations and Internet censorship

Apart from legislation no specific trends in enforcing regulations and Internet censorship were noted.

7.2.11 Trends in Internet related communication surveillance

Apart from a BBC report stating that "Around the world, from Singapore to Saudi Arabia, Internet users find their activities monitored, restricted and sometimes criminalised", (http://news.bbc.co.uk/2/hi/technology/4080886.stm), no specific trends in Internet related communication surveillance were noted.

7.3 POSITIVE TRENDS

7.3.1 Trends in reactions to Internet censorship

Groups supporting artists made an earlier statement that to improve creativity there need to be an end to censorship in Singapore (http://news.bbc.co.uk/2/hi/asia-pacific/2322487.stm).

7.3.2 Attempts and means to side-step Internet censorship

At the time of data mining no attempts and means to side-step Internet censorship were noted.

7.3.3 Trends in cyber actions against Internet censorship

At the time of data mining no trends in cyber actions against Internet censorship were noted.

7.3.4 Trends in innovative ways of showing opposition to Internet censorship

At the time of data mining no trends in innovative ways of showing opposition to Internet censorship were noted.

7.4 CONCLUSION

The evidence with regard to Internet censorship that could be traced through data mining is somewhat in contrast to earlier observations by Amnesty International: "The government of Singapore has a history of using civil defamation actions to stifle political opposition. Such defamation suits place unreasonable restrictions on the right of Singaporeans to peacefully express their opinions and to participate fully in public life" (http://www.amnesty.org/en/news-and-updates/news/singapore-defamation-case-threatens-press-freedom-20091119). From the data presented here it seems as if the focus is on pornography, limited government monitoring and with limited out-speaking against Internet censorship.

7.5 REFERENCES

http://en.wikipedia.org/wiki/Internet_censorship_in_Singapore

http://news.bbc.co.uk/2/hi/asia-pacific/2322487.stm

http://news.bbc.co.uk/2/hi/technology/4080886.stm

http://opennet.net/blog/2005/10/singapore-blocks-gay-web-site

http://opennet.net/blog/2005/09/internet-filtering-singapore-2004-2005;

http://opennet.net/news/singapore-censorship-review-panel-wants-give-parents-more-control-over-childrens-internet-tv-ex

http://opennet.net/policing-content-quasi-public-sphere

http://opennet.net/research/profiles/singapore

http://opennet.net/research/profiles/singaporehttp://en.wikipedia.org/wiki/Internet_censorship_in_Singapore;

http://opennet.net/studies/singapore

http://opennet.net/studies/singapore#toc2e

http://www.amnesty.org/en/library/asset/POL10/001/2011/en/519da037-1492-4620-9ed5-cac8f1cfd591/pol100012011en.pdf

http://www.amnesty.org/en/news-and-updates/news/singapore-defamation-case-threatens-press-freedom-20091119

http://www.browsys.com/search/index.php?ref=self&side=top&q=censorship+and+the+internet%3A+a+singapore+perspective

http://www.efa.org.au/Campaigns/compareasia.html

8 TURKEY

8.1 INTRODUCTION

Although there has been considerable growth in Internet and mobile-telephone use in Turkey over the last few years, there are still problems in some parts of the country, particularly the southeast. The country claims to focus on pornographic content to "protect families", but there are many complaints by the Turkish society about what is considered as disguised Internet censorship and even incidents of "ridiculous" practices have been raised (http://www.euractiv.com/enlargement/turkey-slammed-ridiculous-internet-censorship-news-504608). Reporters Without Borders has added Turkey and Russia to their "under surveillance" list published in the latest report on 12 March 2012 (http://www.bianet.org/english/freedom-of-expression/120653-internet-censorship-turkey-under-surveillance-of-rsf).

Internet censorship in Turkey will be discussed under negative as well as positive trends. The discussion is based on mining a wide variety of Internet resources. There may, however, be many more trends than noted here, as well as many more examples of each. Each individual trend might also be mined in more depth to give a true reflection for the country.

8.2 NEGATIVE TRENDS

8.2.1 Trends in issues of Internet related privacy

At the time of data mining no specific incidents related to issues of Internet privacy were noted.

8.2.2 Ubiquitous society and control

At the time of data mining very little was noted with regard to reports to ubiquitous society and control. Internet service providers (ISPs) are held responsible for blocking access to illegal Web content – even before such blocking has been called for by a court (http://opennet.net/research/profiles/turkey).

8.2.3 Trends in Internet related media being censored

At the time of data mining no specific reports on trends in Internet related media being censored were noted.

8.2.4 Trends in filtering and blocking Internet content and blocking software

In November 2011 Turkey launched a new centralized filtering system “for the safe use of the Internet” under the auspices of its Information Technologies and Communications Authority (BTK). This led to strong reactions in the country as well as from abroad in-spite of the fact that its introduction, initially planned for 22 August 2011, was postponed three months to allow for the plans to be submitted for public consultation (http://en.rsf.org/turkey-turkey-12-03-2012,42065.html**)**.

Turkey allows the blocking of websites that contain certain types of content, including websites deemed to insult Mustafa Kemal Atatürk (also known as the father of modern Turkey). In the case of domestically hosted websites, a website is closed if the content is considered unsuitable. Websites hosted abroad are blocked and filtered through the Internet service providers (ISPs) if the content is considered unsuitable. There seems to be no transparency in decisions which makes it very difficult to appeal against decisions (http://www.freedomhouse.org/article/promises-we-keep-online-internet-freedom-osce-region).

Although the government had a hands-off approach to regulation of the Internet until 2001, there is currently a trend towards considerable legal steps to limit access to certain information, including some political content. To get an indication of the blocking of Internet content: at some stage is was reported that Turkey had banned the YouTube video website for over two years because of videos denigrating Mustafa Kemal Atatürk, and that at the time the Turkish Telecommunications Directorate (TIB) had banned more than 70,000 (mostly pornographic) websites (http://www.eurasianet.org/node/63724). Another report refers to the banning of about 3,700 websites for what was considered mostly "arbitrary and political reasons". The majority of these websites were of foreign origin, dealing with the Kurdish question or aimed at homosexual communities (http://www.bianet.org/english/freedom-of-expression/120653-internet-censorship-turkey-under-surveillance-of-rsf). It was estimated that there were over 5,000 blocked websites as of July 2010; estimates including pornographic websites were much higher (http://www.freedomhouse.org/article/promises-we-keep-online-internet-freedom-osce-region).

Examples of websites being blocked in 2011 and early 2012 include the media streaming service Livestream, pastebin.com, popular file sharing services Rapidshare.com and Fileserve.com, Wix.com (a popular website builder owned by an Israeli company), Blogspot (based on a request by the satellite television provider Digiturk; according to Digiturk Blogger was being used to distribute material it holds the broadcast rights to), as well as Google Apps hosted websites, including all Google App Engine powered websites and some of the Google services. In 2010 even Google Docs, Google Translate, Google Books, Google Analytics, and Google Tools was reported to be banned (http://en.wikipedia.org/wiki/Internet_censorship_in_Turkey#Internet_censorship).

8.2.5 Trends in technologies to monitor and identify citizens using the Internet to express their opinion and applying "freedom of speech"

In 2011 it was reported that the Turkish government agency, Information Technologies Board (BTK) also referred to as the Information Technologies and Communications Authority, or Turkey's Internet watchdog(http://en.rsf.org/turkey-government-agency-wants-to-install-06-05-2011,40238.html; http://www.todayszaman.com/news-252787-turkey-backtracks-on-controversial-internet-filtering-plans.html). According to the planned regulation (Procedures and Principles Regarding the Safe Use of the Internet), Internet users will have to choose between one of four Internet filtering options, namely: family, children, domestic or standard. One of these filters will have to be installed on every computer for it to have online access. The list of websites blocked by each filter is classified. This was met with concern from those who thought that it would place Turkey among the world's top Internet-censoring countries (http://en.rsf.org/turkey-government-agency-wants-to-install-06-05-2011,40238.html; http://www.todayszaman.com/news-252787-turkey-backtracks-on-controversial-internet-filtering-plans.html).

8.2.6 Criminalization of legitimate expression

Some actions against large scale nationwide protests against Internet filters were noted, including the arrest of 32 people, including nine minors. They were suspected of planning attacks on state-run websites as protest to the planned use of Internet filters. Although they were all released they had at the time of the report, pending charges against them under Turkey's anti-terror laws (http://www.eurasianet.org/node/63724).

8.2.7 Trends in acts, regulations and legislation regarding use of the Internet or trends in government models regarding Internet censorship

A report in *Freedom on the Net 2011 by* Freedom House notes that government censorship of the Internet, including some political content, is quite common in Turkey. Furthermore it seems to be on the rise – an impression strengthened by plans for mandatory filtering on all computers used by the public.

Law No. 5651 (also known as the Internet Law of Turkey) was set in motion by the Turkish government in May 2007 to regulate crimes committed via the Internet (http://www.freedomhouse.org/article/promises-we-keep-online-internet-freedom-osce-region).

Other bodies of control include the older media control and censorship association, RTÜK, and a new governmental association, Telecommunication and Transmission Authority. They are allowed to ban Internet websites without prior judicial approval, on the following conditions: "(i) if the offending Web site hosts content that is illegal under Turkish law and is hosted outside Turkey, or (ii) a Web site contains sexual abuse of children or obscenity and its host resides in Turkey". They also focus on crimes against Mustafa Kemal Atatürk, the offering or promotion of prostitution, provision of place and opportunity for gambling, unauthorized online gambling and betting, sexual abuse of children, encouragement of suicide, supplying of drugs that are dangerous for health, and facilitation of the abuse of drugs. In addition they may block websites for the following: downloading of MP3 and movies in violation of copyright laws, insults against state organs and private persons, crimes related to terrorism, violation of trademark regulations, unfair trade regulated under the Turkish Commercial Code, violation of Articles 24, 25, 26, and 28 of the Constitution (freedoms of religion, expression, thought, and freedom of press). It is the responsibility of the Telecommunications Authority to identify the actor(s) responsible for offensive content on the Internet (http://opennet.net/research/profiles/turkey).

In addition to Internet specific legislation, Turkey also has a legal framework that regulates the freedom of expression and freedom of press. This consists of the Press Law and the Law on the Establishment of Radio and Television Enterprises and Their Broadcasts (the RTUK Law). The 2004 Press Law No. 5187 annulled the former Press Law No. 5680 and its amendments, which brought Internet broadcasting under the press legislation, which meant that websites and Internet service providers' monitoring standards were criticized for being incompatible with the characteristics of the Internet (http://opennet.net/research/profiles/turkey).

Turkish courts have also been noted to base their decisions on blocking access on violations of other crimes and even some private law rules. Based on statistics from Turk Telecom banned websites based on norms other than Article 8 of Internet Law No. 5651, numbered 153 in 2005, 886 in 2006, and 549 in 2007 (http://opennet.net/research/profiles/turkey).

8.2.8 Trends in new forms of Internet censorship

At the time of data mining no trends on new forms of Internet censorship were noted.

8.2.9 Trends in support of Internet censorship

Following attacks in Norway in 2011, the Turkish Deputy Prime Minister, Bülent Arinç, stated that the attacks justify the government's plans to implement an Internet filtering system. Apparently he argued that the Breivik attacks were aided by the Internet (http://opennet.net/blog/2011/08/europe-responds-norway-attacks-calls-internet-monitoring-emerge).

In 2008 Google decided to selectively prevent access to the offending videos on YouTube to users in Turkey to prevent the entire YouTube website from being blocked. Turkish prosecutors demanded a global block in order not to offend Turkish users abroad; Google did not comply to this (http://en.wikipedia.org/wiki/Internet_censorship_in_Turkey#Internet_censorship).

8.2.10 Trends in enforcing regulations and Internet censorship

Several websites that backed anti-censorship demonstrations held on 15 May 2011 have been intermittently inaccessible since then because of Distributed Denial of Service (DDoS) attacks. These websites include the left-wing daily *Birgün*, the news website haber.sol.org.tr and the media freedom website Bianet (http://en.rsf.org/turkey-government-agency-wants-to-install-06-05-2011,40238.html).

8.2.11 Trends in Internet related communication surveillance

Turkey has one main commercial backbone connection, owned and controlled by Turk Telecom and the educational network, UlakNet. Most of the filtering of international Internet traffic takes place on the Turk Telecom network, which links to other commercial Internet service providers within the country. According to the OpenNet Initiative it seems as if the academic network in Turkey did not, at the time of their testing, engage in Internet filtering. UlakNet primarily provides Internet access to academic centers and some government institutions, including the military (http://opennet.net/research/profiles/turkey).

8.3 POSITIVE TRENDS

8.3.1 Trends in reactions to Internet censorship

It was reported that more than 10,000 people took part in demonstrations on 15 May 2012 against online censorship. These demonstrations were held in Istanbul and around 30 other Turkish cities. The demonstrations were against changes to media and Internet censorship legislation that would enforce the installation of online filtering software on all home computers (http://en.rsf.org/turkey-government-agency-wants-to-install-06-05-2011,40238.html).

8.3.2 Attempts and means to side-step Internet censorship

It seems that blocked websites are however, often, due to the lack of juridical, technical, or ethical arguments to justify the censorship, still available by using proxies or by changing DNS servers (http://en.wikipedia.org/wiki/Internet_censorship_in_Turkey#Internet_censorship).

8.3.3 Trends in cyber actions against Internet censorship, e.g. cyber and virtual demonstrations and protest

Street demonstrations against Internet censorship have been noted with special reference to the demonstrations in May and June 2011 when tens of thousands of people joined nationwide protests against the current government's decision to introduce a nationwide compulsory Internet filtering system on all home computers (http://www.freedomhouse.org/article/promises-we-keep-online-internet-freedom-osce-region). There was also a report on an online activist group, Anonymous, that has issued a threat to the Turkish government in response to the proposed filtering system (http://opennet.net/blog/2011/06/anonymous-turkish-government-over-censorship-%E2%80%9Cexpect-us%E2%80%9D). In reaction to Distributed Denial of Service (DDoS) attacks, and being shut down for several hours, Bianet, a media freedom website issued a statement: "We are going to carry on publishing under alternative addresses in case we should become the subject of similar attacks in the future"… "If this should occur, the alternative address will be published on Twitter and via other channels" (http://en.rsf.org/turkey-government-agency-wants-to-install-06-05-2011,40238.html).

In mid-2008 a protest campaign organised by the website elmaaltshift.com, which encouraged websites to replace their home page with an interstitial webpage titled "Access To This Site Is Denied By Its Own Decision" were reported (http://en.wikipedia.org/wiki/Internet_censorship_in_Turkey#Internet_censorship).
The Alternative Informatics Association (Alternatif Bilişim) has also been reported to criticise the closure of Internet websites, calling for Internet users to protest to the Telecommunications Department by fax, email and telephone and for those who have websites on GoogleSites to protest, too. They offered legal advice and support in helping people to write legal letters of objection and taking on legal actions or other actions (http://www.bianet.org/english/freedom-of-expression/115559-googlesites-hit-by-turkeys-censorship). It seems as if "Despite relentless pressure, netizens have been mobilizing against the implementation of backdoor censorship on the Web" (http://en.rsf.org/turkey-turkey-12-03-2012,42065.html; http://en.rsf.org/turquie-new-internet-filtering-system-02-12-2011,41498.html).

8.3.4 Trends in innovative ways of showing opposition to Internet censorship

At the time of data mining no reports were noted on innovative ways of showing opposition to Internet censorship.

8.4 CONCLUSION

Although there is some concerns about the Turkish government's control of Internet access for much more than moral reasons (e.g. pornography), it seems not to be as harsh as in countries such as China and Myanmar. Data mining also picked up more reports on expressions of opinion by the public on Internet censorship.

8.5 REFERENCES

http://en.rsf.org/turkey-government-agency-wants-to-install-06-05-2011,40238.html

http://en.rsf.org/turkey-turkey-12-03-2012,42065.html

http://en.rsf.org/turkey-turkey-12-03-2012,42065.html; http://en.rsf.org/turquie-new-internet-filtering-system-02-12-2011,41498.html

http://en.wikipedia.org/wiki/Internet_censorship_in_Turkey#Internet_censorship

http://opennet.net/blog/2011/06/anonymous-turkish-government-over-censorship-%E2%80%9Cexpect-us%E2%80%9D

http://opennet.net/blog/2011/08/europe-responds-norway-attacks-calls-internet-monitoring-emerge

http://opennet.net/research/profiles/turkey

http://www.bianet.org/english/freedom-of-expression/115559-googlesites-hit-by-turkeys-censorship

http://www.bianet.org/english/freedom-of-expression/120653-internet-censorship-turkey-under-surveillance-of-rsf

http://www.bianet.org/english/freedom-of-expression/120653-internet-censorship-turkey-under-surveillance-of-rsf

http://www.euractiv.com/enlargement/turkey-slammed-ridiculous-internet-censorship-news-504608

http://www.eurasianet.org/node/63724

http://www.freedomhouse.org/article/promises-we-keep-online-internet-freedom-osce-region

http://www.todayszaman.com/news-252787-turkey-backtracks-on-controversial-internet-filtering-plans.html

9 UNITED KINGDOM

9.1 INTRODUCTION

In April 1994 it was reported that Britain already had “some of the toughest censorship rules for films and videos in the world…”, and that it seemed as if these will be further tightened (http://www.independent.co.uk/news/uk/censorship-laws-among-toughest-in-the-world-1367469.html). There have been an increasing number of censorship cases in the United Kingdom (UK). For instance, in February 2012, members of the United Kingdom Parliament on concluding that the Internet plays a major role in the radicalization of terrorists, called on the government to pressure Internet service providers in Britain and abroad to censor online speech (http://www.browsys.com/search/?q=Pakistan+censorship).

Internet censorship in the United Kingdom will be discussed under negative as well as positive trends. The discussion is based on mining a wide variety of Internet resources. There may be many more trends than noted here, as well as many more examples of each. Each trend still needs to be studied in more detail.

9.2 NEGATIVE TRENDS

9.2.1 Trends in issues of Internet related privacy

It seems as if there are various measures in the United Kingdom to monitor for illegal content that might be seen as a breach of privacy. The use of deep-packet inspection technology (DPI) involves looking at the contents of data packets. This technology has been linked to T-Mobile practices to enforce contractual terms such as 'fair-use' agreements, as well as for the enforcement of other terms and conditions. In January 2012, it was reported that T-Mobile admitted that it intercepted secure email sent from its customers' mobile phones for over three months as the result of a technical error (http://www.zdnet.co.uk/news/security-threats/2012/01/12/t-mobile-we-intercepted-secure-email-from-phones-40094794/). In February 2012 there was a report on an investigation by the FBI on how activists linked to the Anonymous network managed to intercept a conference call between British and United States police in which they discussed legal action against hackers (http://www.bbc.co.uk/news/world-us-canada-16881582).

Since 1 August 1996 JANET (UK) was responsible for the administration and registration of domain names under the ac.uk and gov.uk domains. Commercial Internet service providers in the United Kingdom may apply for a Registrar Membership Account with JANET. The government’s fear for cyber-attacks on vital computer networks has been noted as a "new and growing threat" to the security of the United Kingdom. At the time (October 2010) it was noted that more than half of all the identified computer attacks up to the time were made in 2009 (http://news.bbc.co.uk/today/hi/today/newsid_9101000/9101076.stm).

9.2.2 Ubiquitous society and control

The Police Central e-crime Unit (PCeU) is jointly funded by the Home Office and Metropolitan Police to respond to the most serious incidents of cyber-crime at a national level. Their vision reads: "To contribute, alongside national and international partners, towards the provision of a safer and more secure cyber environment, in support of the National Cyber Security Strategy, that enhances trust and confidence in the UK as a place to live and conduct business" (http://www.met.police.uk/webinfo/index.htm#copyright).

Some of the actions of the government are interpreted as using journalists to gain access to information that may reflect issues of national security. This is clear from a report by Index on Censorship appearing in 2011, expressing concern about the fact that news organisations are expected to hand over footage of the riots in August 2011 in England. Their report states: “Moves such as this force journalists to become the eyes and ears of the state… During the riots, we saw several incidents of photographers and broadcasters being attacked. The implication that any footage taken by them will be handed over to authorities will only serve to endanger on-the-ground media workers further in the future.” Such footage may appear in the printed media or on the Internet, and is therefore mentioned here as part of Internet censorship (http://www.indexoncensorship.org/2011/09/uk-media-should-not-be-forced-to-hand-over-riot-footage/).

9.2.3 Trends in Internet related media being censored (text, audio, video, Usenet groups, social media, etc.)

Various reports on media being monitored were noted amongst others, YouTube and other media. This was met with outcries of “The UK government's plans to censor social media are idiotic and dangerous” (http://articles.businessinsider.com/2011-08-11/europe/29992150_1_burka-ban-social-media-rioters#comments). There were even comparisons to what is happening in China. Although reports on television censorship are not Internet related, it gives an indication of the scope of monitoring and censorship in the United Kingdom and the rationale for concern about censorship (http://www.youtube.com/watch?v=JaWJtpZdoew&feature=related; http://www.youtube.com/watch?v=61_O2IO42KQ&feature=related; http://www.youtube.com/watch?v=d4x_wcS6NN0&feature=related; http://www.presstv.ir/detail/222180.html_).

In November 2008 a report appeared on the monitoring of the media with regard to national security. It read “Britain's security agencies and police would be given unprecedented and legally binding powers to ban the media from reporting matters of national security, under proposals being discussed in Whitehall. The committee also wants to censor reporting of police operations that are deemed to have implications for national security" (http://www.independent.co.uk/news/uk/politics/mps-seek-to-censor-the-media-1006607.html).

Although the British Prime Minister, David Cameron, proposed a ban on social media at the time of wide-scale unrest in England in early August 2011, the United Kingdom Government decided to drop the idea to ban the use of social media (http://opennet.net/blog/2011/09/uk-government-drops-plans-ban-social-media). It, however, seems that the United Kingdom will sharpen its "cyber-security" strategy aimed at social networks such as Facebook and Twitter (https://www.eff.org/deeplinks/2011/12/week-internet-censorship--good-news-bad-news).

It has also been noted that censorship of motion pictures, video games and Internet websites hosted in the United Kingdom are considered to be among the strictest in the European Union (http://en.wikipedia.org/wiki/Censorship_in_the_United_Kingdom).

In 2012 the Open Rights Group called on mobile operators to give parents an "active choice" to turn filters on. They also requested mobile operators to be more transparent about how their systems work (http://www.afterdawn.com/news/article.cfm/2012/05/16/report_slams_mobile_internet_censorship_in_uk).

9.2.4 Trends in filtering and blocking Internet content and blocking software

Although the United Kingdom does not seem to have a specific law on Internet censorship, all major domestic broadband companies seems to pass Internet traffic through a filter with the intention to identify websites thought to contain indecent images of children. A blacklist of such websites is compiled by the Internet Watch Foundation (an independent organisation) (http://news.bbc.co.uk/newsbeat/hi/technology/newsid_7264000/7264277.stm). This may lead to websites being blocked (http://en.wikipedia.org/wiki/Internet_censorship_in_the_United_Kingdom). The Internet Watch Foundation uses the services of police-trained analysts to compile the blacklist. It has been claimed that they can add an average of 65-80 new URLs to the list each week (http://en.wikipedia.org/wiki/Internet_censorship_in_the_United_Kingdom). The analysts react to reports from the public and are not merely pursuing their own interests and interpretation of what qualifies as child pornography (http://en.wikipedia.org/wiki/Internet_censorship_in_the_United_Kingdom). Incidents of requests to Internet Watch Foundation have been reported e.g. their decision to blacklist a web page with a naked and possibly underage female on the cover of a 1976 album from German rock group The Scorpions titled "Virgin Killer" (http://www.cio.com/article/470014/U.K._Wikipedia_Blacklisting_Dropped; http://www.pcworld.com/article/155112/wikipedia_article_censored_in_uk_for_the_first_time.html).

On the Internet Watch Foundation's website they state the following about their service and functionality: "The IWF's 'notice and takedown' service is central to our existence and concerns the systematic removal of content within our remit from UK networks. Any content assessed by our Internet Content Analysts as child sexual abuse, non-photographic child sexual abuse images or criminally obscene adult content which is hosted in the UK is swiftly removed at source following a notice from the IWF to the hosting provider. This process is carried out in partnership with the relevant police agency to ensure any relevant evidence is preserved. This process has operated since 1996 and is UK-wide. As a result the volume of UK-hosted child sexual abuse content has reduced from 18% of the total known to the IWF in 1997 to less than 1% since 2003" (http://www.iwf.org.uk/services/removal).

Testing by the OpenNet Initiative in 2010 found no evidence of technical filtering in the political, social, conflict/security, or Internet tools areas; they does, however, not test for the blocking of child pornography, to which the United Kingdom openly admits. There are also laws in the United Kingdom against the publication or possession of certain material such as child pornography (http://en.wikipedia.org/wiki/Internet_censorship_in_the_United_Kingdom).

The British Telecommunications Internet service provider uses a specialist service, Cleanfeed, for Internet filtering. This service uses data provided by the Internet Watch Foundation to identify web pages that might contain indecent photographs of children. If Cleanfeed finds such a page, it creates a "URL not found" error page rather than deliver the actual page or a warning page (http://en.wikipedia.org/wiki/Internet_censorship_in_the_United_Kingdom). Internet service providers in the United Kingdom, however, do not all use the same filtering systems. Apart from Cleanfeed, reference to WebMinder was also noted (http://en.wikipedia.org/wiki/Internet_censorship_in_the_United_Kingdom).

A report appearing 23 February 2009 claimed that it is suggested that 95% of Internet access in the United Kingdom is censored, and more specifically that only 5% of Internet access is not filtered using the Internet Watch Foundation blacklist (http://aaisp.net.uk/news-censorship.html). In November 2011 a report appeared on users from the United Kingdom not having access to the popular Fileserve file-hosting service. (Fileserve is one of the 10 most-visited file-sharing sites on the Internet. It allows users to store files in the cloud for personal use or subsequent sharing with the rest of the world.) (http://torrentfreak.com/uk-internet-blacklist-censors-fileserve-file-hosting-service-111118/). In October 2011 British Telecommunication was ordered to block Newzbin2, a filesharing website due to the fact that the website was considered to promoting illegal filesharing. It seems as if complaints came from various Hollywood studios, such as Warner Bros, Paramount, Disney, and Universal (http://opennet.net/news/bt-ordered-block-newzbin2-filesharing-site-within-14-days; http://www.guardian.co.uk/technology/2011/oct/26/bt-block-newzbin2-filesharing-site; http://opennet.net/blog/2011/11/threats-open-net-november-4-2011).

In April 2012 *The Guardian* reported that "A cross-party committee of MPs and peers has urged the government to consider introducing legislation that would force Google to censor its search results to block material that a court has found to be in breach of someone's privacy. By "privacy", they were referring to the so-called "super-injunctions" – censorship orders, usually taken out by celebrities or wealthy individuals, which ban a publisher from mentioning a topic or even the injunction" (http://www.aljazeera.com/indepth/opinion/2012/04/201241373429356249.html). Reports such as these seem to reflect an increasing urgency in the United Kingdom to sharpen surveillance of communication and Internet censorship.

9.2.5 Trends in technologies to monitor and identify citizens using the Internet to express their opinion and applying "freedom of speech" e.g. activists, critics

In 2011 a report appeared that the United Kingdom intends to introduce surveillance technology that can inform authorities if banned users are "breaking the bail or sentencing conditions that have been set on their Internet use" (https://www.eff.org/deeplinks/2011/12/week-internet-censorship--good-news-bad-news).

9.2.6 Criminalization of legitimate expression (e.g. thoughts, ideas, arguments) on the Internet

A number of incidents of legal and other actions regarding censorship, file sharing, etc. in the United Kingdom were reported. It seems as if there have been an increasing number of censorship cases in the United Kingdom.

The file-sharing website, The Pirate Bay, was reported in February to have been ruled illegal by the High Court in London. The Court argued that the website is guilty of the massive breach of copyright. According to the report the ruling is paving the way for blocking at the Internet service provider level to be enacted when a final judgement is made (which was according to the report, expected to be in June) (http://www.zdnet.com/blog/london/sleepwalking-into-censorship-pirate-bay-faces-uk-web-block/3171). This followed the filing for a lawsuit by several music corporations including EMI and Sony against the website after appealing to the Copyright, Designs and Patents Act (http://opennet.net/blog/2012/05/threats-open-net-may-4-2012).

In May 2012 the police arrested a Newcastle teenager suspected of belonging to the Team Poison hacker group. This followed two days after the arrest of two teenagers in Norway in connection with a series of cyber attacks which included an attack on the United Kingdom website, Serious Organised Crime Agency (SOCA). According to the report Team Poison, has in April 2012 already been linked to more than 1,000 offences; in April 2012 they claimed responsibility for hacking into the phone system of the counter-terrorism unit of Scotland Yard (http://www.computerweekly.com/news/2240150117/Police-arrest-suspected-TeamPoison-hacker).

In April 2012 a report appeared on a 21-year-old college student being sentenced in Swansea to 56 days in jail for a series of "racially offensive" written tweets on a popular football player, Fabrice Muamba who had collapsed from cardiac arrest during a game in March (http://www.aljazeera.com/indepth/opinion/2012/04/201241373429356249.html). The district judge, after calling the comments “vile and abhorrent,” told the student, "I have no choice but to impose an immediate custodial sentence to reflect the public outrage at what you have done.”

9.2.7 Trends in acts, regulations and legislation regarding use of the Internet and trends in government models regarding Internet censorship

Initially the United Kingdom did not have legislation concerning Internet censorship. They did, however, had legislation against pornography, especially child pornography, and the protection of Children e.g. the United Kingdom’s Protection of Children Act 1978. In April 2010 it was reported that the United Kingdom Parliament passed a controversial Digital Economy Bill, which gave new powers to control access to the Internet (https://www.eff.org/deeplinks/2010/04/u-k-passes-internet-disconnection-law). Other legislation that need to be noted with regard to interception of communications is the Regulation of Investigatory Powers Act 2000 (“RIPA”), and The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002.

The Data Retention (EC Directive) Regulations of 2009 give the requirements that notified communication providers have to adhere to when required to retain call data records and/or other information. The information should reflect the extent of the network or service provided to a customer for a period of 12 months from when it was created (http://robbratby.com/uk-telecoms-law/interception-and-data-retention-for-telecoms-in-the-uk/).

At the time a committee of the United Kingdom’s Members of Parliament also investigated the Internet's role in compromising Britain's privacy laws. They recommended that Google should be ordered to censor its search results for British people, to prevent the “tittle-tattle about the love-lives of celebrities and oligarchs (as well as the criminal misdeeds of giant corporations)” to be discovered. They also expected advertisers to pull their advertisements from websites and newspapers that refuse the "voluntary" code of conduct that demands the media “kowtow” to the courts' secrecy orders (http://boingboing.net/2012/03/26/uk-mps-recommend-laws-compelli.html).

Under section one of the Regulation of Investigatory Powers Act (RIPA) 2000 it is on the other hand an offence to intercept any communication, such as letters or emails when it is transmitted. This prohibit anybody other than the sender or intended recipient to have access to the communication while transmitted, that is until it is opened by the recipient.
RIPA provides exceptions to this rule (circumstances in which it will not be a criminal offence to intercept an email), the most notable of which is an interception warrant. “In England and Wales only the home secretary can issue such a warrant and he can only do so if he believes that the warrant is necessary in the interests of national security, for the purposes of preventing or detecting serious crime or to safeguard the economic well-being of the UK (but only from people outside the country), and that the conduct the warrant authorises is proportionate to what it hopes to achieve”.

The heads of bodies such as the various security services, the police, the Serious Organised Crime Agency (and its Scottish equivalent) and HM Revenue and Customs may apply for such warranties. The Interception of Communications Commissioner oversees the issue of such warrants and interception activities (http://www.guardian.co.uk/commentisfree/libertycentral/2009/aug/24/surveillance-email).

From 26 May 2012 a “cookie law” will be enforced expecting website owners to ensure the websites obtain users' opt-in consent first if they want to install pieces of code, known as "cookies", that store and pass on personal details and information about browsing activities to third parties, or risk fines of up to £500,000. This regulation comes from an amendment to the European Union's Privacy and Electronic Communications Directive. The intention with the regulation is to ensure that websites provide "clear and comprehensive" information about the use of cookies (http://www.computerweekly.com/news/2240150407/Most-UK-government-websites-to-miss-cookie-law-deadline).

9.2.8 Trends in new forms of Internet censorship, e.g. Halaal Internet, implied censorship such as user rating

At the time of data mining no reports on new forms of Internet censorship were noted.

9.2.9 Trends in support of Internet censorship, e.g. computer and Internet companies, search engines, Internet service providers

Voluntary Internet filtering was done since June 2004 when the Cleanfeed filtering program was introduced into the United Kingdom. This was especially endorsed by British Telecommunications the largest Internet service provider. Data obtained from the Internet Watch Foundation is used to identify pages suspected to contain indecent photographs of children (http://en.wikipedia.org/wiki/Censorship_in_the_United_Kingdom).

Internet service providers, mobile network operators, content providers and search engines e.g. Google and Yahoo are provided with a copy of the censorship list compiled by the Internet Watch Foundation. They are encouraged to block access to websites on this list. People who try to get access to illegal content hosted overseas get an error message. The
United Kingdom's Child Exploitation and Online Protection Centre also participate in Internet surveillance, and the police are legally allowed to forward the personal details of people who have accessed illegal content to banks, who "will cancel their credit cards as a breach of service" (http://www.scribd.com/doc/24138351/Untangling-the-Net-The-Scope-of-Content-Caught-by-Mandatory-Internet-Filtering#page=23).

In May 2012 suggestions by the British defence secretary, Jim Murphy, was reported. He argued that a mix of regulation and education, in combination with a "hard-hitting advertising campaign" should be used to raise public awareness about threats. This might also encourage people to take more care when using the Internet (http://www.computerweekly.com/news/2240150318/Tackle-cyber-security-with-hard-hitting-ad-campaign-says-Labour).

9.2.10 Trends in enforcing regulations and Internet censorship

At the time of data mining no specific trends on data mining were noted.

9.2.11 Trends in Internet related communication surveillance

In an open letter to Members of Parliament on Internet surveillance (May 2012), Reporters Without Borders expressed their concern on a Bill on the surveillance of electronic and telephone communications, namely the Communications Capabilities Development Programme. The intention of the Bill is to extend the surveillance of the electronic and telephone communications of British citizens (http://en.rsf.org/united-kingdom-open-letter-to-members-of-11-05-2012,42605.html).

The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002 (RIPA) determines the circumstances under which certain Internet service providers are required to intercept communications. The intention with RIPA is to maintain a balance between the rights of the state and individuals; it also covers non electronic communication services.

Under RIPA the Secretary of State can expect the "public telecommunications service" providers to put in place and maintain certain interception capabilities, and may serve warrants on such services to require interception of communications (http://robbratby.com/uk-telecoms-law/interception-and-data-retention-for-telecoms-in-the-uk/).

A mass surveillance plan was strongly defended by British Prime Minister, David Cameron, in April 2012. This plan would allow the government to monitor every email, text message and phone call throughout the country. According to the plan, Internet service providers would be forced to install hardware that would give law enforcement real time, on-demand access to every Internet user's IP address, email address books, when and to whom emails are sent and how frequently. This would also apply to phone calls and text messages. If this goes through “Censorship and surveillance proposals would put the UK's approach to internet freedom on par with authoritarian regimes” (http://www.aljazeera.com/indepth/opinion/2012/04/201241373429356249.html). After the plans were compared with the plans implemented by Egypt, it did not materialise. It still seems as if the government is considering a serious of legislation that would limit online privacy and freedom of speech (http://www.aljazeera.com/indepth/opinion/2012/04/201241373429356249.html).

Reports on the so called 'snoopers charter' also appeared in 2012. This would force Internet service providers to install hardware to allow the government access to online communications and to keep records of all emails, messages on social networking sites and conversations via Skype. It would allow monitoring in “real time” (http://www.aljazeera.com/programmes/insidestory/2012/04/2012448816173111.html).

9.3 POSITIVE TRENDS

9.3.1 Trends in reactions to Internet censorship: changes in groups, group dynamics, responses and actions of groups

In March 2011 *The Guardian UK* reported that the BBC World Service has asked the United States government for funding to combat censorship in Iran and China. The report further indicated that the United States State Department planned to provide an amount in the “low six-figures” to the international broadcasting arm of the BBC to further develop anti-jamming technology and proxy servers that can circumnavigate these countries’ attempts to censor the BBC’s content (http://opennet.net/blog/2011/03/bbcs-application-us-state-department-funding-draws-american-criticism).

In April 2012 the hacking group Anonymous was reported to threat to launch online attacks every weekend. This followed on claims that it disrupted access to the Home Office website. Amongst other things Twitter messages were used: "Expect a DDoS (distributed denial-of-service) every Saturday on the UK Government sites." (http://www.bbc.co.uk/news/uk-17648852). In another threat they state that they would stop the Internet on 31 March, using the phrase "Operation Blackout". Those issuing the threat even went so far as to state how they would do it, i.e. by disabling the Domain Name Service (DNS) (http://www.bbc.com/news/technology-17472447).

In May 2012 the Open Rights Group (ORG) and the LSE Media Policy Project released a report which showed serious over-blocking of websites as a result of the Internet filters used in the United Kingdom. The groups found that the filters led to the incorrect blocking of political commentaries, personal blogs, restaurants' sites and community websites. Their report requested mobile operators to give parents an “active choice” to turn filters on, and to be more transparent about how their systems work (http://www.afterdawn.com/news/article.cfm/2012/05/16/report_slams_mobile_internet_censorship_in_uk).

According to a report in November 2011 the British Foreign Secretary, William Hague, opposed the United Kingdom government's plans for Internet censorship for security purposes at the London Conference on Cyberspace (http://opennet.net/news/britain-decries-internet-censorship).

Although it is not necessarily in support of Internet censorship, Danvers Baillieu, a specialist in Internet law, made the following remark with regard to the “Snoopers Charter” the United Kingdom government is planning: "Any terrorist who is seriously trying to do harm to people, they are going to be taking all sorts of counter-measures to hide their tracks and this sort of law is really not going to get you anywhere." (http://www.aljazeera.com/programmes/insidestory/2012/04/2012448816173111.html)

9.3.2 Attempts and means to side-step Internet censorship

According to the Internet Watch Foundation’s 2011 Annual Report criminals are “disguising” websites to appear as if they host only legal content. However, if an Internet user follows a predetermined digital path which leads them to the website, they will see images and videos of children being sexually abused. During 2011 the used of this technique was noted almost 600 times (http://www.iwf.org.uk/about-iwf/news/post/321-internet-watch-foundation-report-highlights-new-abuse-of-online-technology).

9.3.3 Trends in cyber actions against Internet censorship

In February 2012 strong opposition to the Anti-Counterfeiting Agreement (Acta) have been noted across Europe, as well as in London. A petition was launched calling for the rejection of the agreement. It got more than 1.75 million signatures. Activism website, stopp-acta.info lists more than 100 protests scheduled across Europe (http://www.computerweekly.com/news/2240114878/UK-to-take-part-in-weekend-protests-against-ACTA).

9.3.4 Trends in innovative ways of showing opposition to Internet censorship

Strong criticism of the government's plans for surveillance appeared in the British media e.g. as reported by *The Guardian*: "As usual, the government and HMRC public relations people underplay the wide-ranging and dangerous nature of this proposal by insisting that the new measure is simply designed to deal with the problem of tobacco smuggling. But the change, disclosed in a document published with the budget, means that HMRC will be able to trawl through private mail pretty much at will." (http://www.guardian.co.uk/commentisfree/henryporter/2010/mar/27/intercepting-mail-stasi-tax-inspectors)

Anonymous is a group of people who come together online, with the intention to protest against censorship and surveillance. It seems to consist of smaller groups of various sizes, and make-up; the composition depends on the particular cause the group is addressing at the time. The members of Anonymous identify themselves in web videos by wearing Guy Fawkes masks or V for Vendetta. The protests often aim to disrupt websites and web services (http://www.thesun.co.uk/sol/homepage/news/4107450/Hackers-intercept-FBI-call-to-Scotland-Yard.html).

In another reported incident, computer hackers, allegedly belonging to Anonymous bugged a conference call between Scotland Yard and the FBI in which they were discussing how "to nail the group". The conversation was then posted online. It is suspected that they picked up the password in an email sent by and FBI agent (http://www.thesun.co.uk/sol/homepage/news/4107450/Hackers-intercept-FBI-call-to-Scotland-Yard.html).

9.4 CONCLUSION

The United Kingdom, like many democratic and liberal states, censors pornographic information. In the process of censoring pornographic information through Internet it has been reported by the Open Rights Group (ORG) that there is widespread over-blocking. The Open Rights Group reported that the filters that are used lead to the incorrect blocking of political commentaries, personal blogs, restaurants' sites and community websites. The United Kingdom's censorship efforts seem to have increased with years and there is evidence that the government is working on structures and institutions, including strategies and regulations on electronic censorship and cyber surveillance as a result of issues such as state security against terrorism and malicious cyber attacks, among others.

9.5 REFERENCES

http://aaisp.net.uk/news-censorship.html

http://articles.businessinsider.com/2011-08-11/europe/29992150_1_burka-ban-social-media-rioters#comments

http://boingboing.net/2012/03/26/uk-mps-recommend-laws-compelli.html

http://en.rsf.org/united-kingdom-open-letter-to-members-of-11-05-2012,42605.html http://en.wikipedia.org/wiki/Internet_censorship_in_the_United_Kingdom

http://news.bbc.co.uk/newsbeat/hi/technology/newsid_7264000/7264277.stm

http://news.bbc.co.uk/today/hi/today/newsid_9101000/9101076.stm

http://opennet.net/blog/2011/03/bbcs-application-us-state-department-funding-draws-american-criticism

http://opennet.net/blog/2011/09/uk-government-drops-plans-ban-social-media

http://opennet.net/blog/2011/11/threats-open-net-november-4-2011

http://opennet.net/blog/2012/05/threats-open-net-may-4-2012

http://opennet.net/news/britain-decries-internet-censorship

http://opennet.net/news/bt-ordered-block-newzbin2-filesharing-site-within-14-days

http://robbratby.com/uk-telecoms-law/interception-and-data-retention-for-telecoms-in-the-uk/

http://torrentfreak.com/uk-internet-blacklist-censors-fileserve-file-hosting-service-111118/

http://www.afterdawn.com/news/article.cfm/2012/05/16/report_slams_mobile_internet_censorship_in_uk

http://www.aljazeera.com/indepth/opinion/2012/04/201241373429356249.html

http://www.aljazeera.com/programmes/insidestory/2012/04/2012448816173111.html

http://www.bbc.co.uk/news/uk-17648852

http://www.bbc.co.uk/news/world-us-canada-16881582

http://www.bbc.com/news/technology-17472447

http://www.cio.com/article/470014/U.K._Wikipedia_Blacklisting_Dropped

http://www.computerweekly.com/news/2240114878/UK-to-take-part-in-weekend-protests-against-ACTA

http://www.computerweekly.com/news/2240150117/Police-arrest-suspected-TeamPoison-hacker

http://www.computerweekly.com/news/2240150318/Tackle-cyber-security-with-hard-hitting-ad-campaign-says-Labour

http://www.computerweekly.com/news/2240150407/Most-UK-government-websites-to-miss-cookie-law-deadline

http://www.guardian.co.uk/commentisfree/henryporter/2010/mar/27/intercepting-mail-stasi-tax-inspectors

http://www.guardian.co.uk/commentisfree/libertycentral/2009/aug/24/surveillance-email

http://www.guardian.co.uk/technology/2011/oct/26/bt-block-newzbin2-filesharing-site

http://www.independent.co.uk/news/uk/censorship-laws-among-toughest-in-the-world-1367469.html

http://www.independent.co.uk/news/uk/politics/mps-seek-to-censor-the-media-1006607.html

http://www.indexoncensorship.org/2011/09/uk-media-should-not-be-forced-to-hand-over-riot-footage/

http://www.iwf.org.uk/about-iwf/news/post/321-internet-watch-foundation-report-highlights-new-abuse-of-online-technology http://www.iwf.org.uk/services/removal

http://www.met.police.uk/webinfo/index.htm#copyright

http://www.pcworld.com/article/155112/wikipedia_article_censored_in_uk_for_the_first_time.html

http://www.presstv.ir/detail/222180.html_

http://www.scribd.com/doc/24138351/Untangling-the-Net-The-Scope-of-Content-Caught-by-Mandatory-Internet-Filtering#page=23

http://www.thesun.co.uk/sol/homepage/news/4107450/Hackers-intercept-FBI-call-to-Scotland-Yard.html

http://www.youtube.com/watch?v=61_O2IO42KQ&feature=related

http://www.youtube.com/watch?v=d4x_wcS6NN0&feature=related

http://www.youtube.com/watch?v=JaWJtpZdoew&feature=related

http://www.zdnet.co.uk/news/security-threats/2012/01/12/t-mobile-we-intercepted-secure-email-from-phones-40094794/

http://www.zdnet.com/blog/london/sleepwalking-into-censorship-pirate-bay-faces-uk-web-block/3171

https://www.eff.org/deeplinks/2010/04/u-k-passes-internet-disconnection-law

https://www.eff.org/deeplinks/2011/12/week-internet-censorship--good-news-bad-news