Internet censorship in South Africa: a brief exposé of negative and positive trends

Constance Bitso[1]
connie.bitso@uct.ac.za
ORCID Id.: https://orcid.org/0000-0003-4727-1257

Received: 14 June 2013
Accepted: 22 June 2014

This article investigates internet censorship in South Africa using a set of negative and positive internet censorship trends adapted from Bitso, Fourie and Bothma (2012) to raise awareness in light of increasing global internet censorship and South Africa's involvement in a proposal for inter-governmental policy on the internet. Both positive and negative internet censorship trends are noted. The investigation reveals that South Africa has the highest level of media freedom in Africa. However, there are three concerns highlighted that might have a bearing on internet censorship in South Africa. Firstly, there is the formulation of legislation that might impact on the use of information, in particular the Protection of State Information Bill (2010). As such, various campaigns and cyber actions were made against this Bill because it is deemed to entrench information censorship. Secondly, there is the hacking of South African government websites, including that of the police on more than one occasion. This warrants internet censorship in order to combat crime as well as to ensure safety and security. Thirdly, there is the increasing challenge of spam and malware that calls for filtering to protect systems such as servers.

Keywords: Internet censorship, South Africa

1 Introduction

The internet has traditionally been a free medium for publishing and accessing information. However, its censorship appears to have spread globally, even in established democracies. In a Group of Eight (G8) meeting in May 2011, for example, France's president at the time, Nicholas Sarkozy, raised issues of piracy and intellectual property rights relating to the internet ("Sarkozy to host…" 2011).The meeting led to a proposal by Sarkozy to strengthen global internet control (Karhula 2011). In August 2011, during the London riots, the British Prime Minister, David Cameron, called for a social media clampdown (Halliday & Garside 2011). In the same year, a proposal to establish an inter-governmental policy forum for the internet was suggested by three of the BRICS nations (India, Brazil and South Africa) at the 6th Annual Internet Governance Forum in Nairobi. In the USA, too, there has been a focus on legislation which could result in possible internet censorship (Wang 2003). Around the world, there have been signs of censoring the internet, particularly social media, as Dick (2012: 260) asserts:

> Australia's mandatory national web-filtering system; Finland's increased internet surveillance for terrorist threats; the UK's internet Censorship and Disconnection Law, and the USA's Stop Online Piracy Act and Protect Intellectual Property Act are some of the technical and legislative mechanisms used to curb the use of the social media.

It seems that "censorship is a real and vast problem that affects people in every country even in established democracies such as the United States" (Epstein 2014).

Although the internet offers numerous opportunities and advantages with regard to increased access to information and empowering people (Witschge 2008), it has become a popular tool for repression, censorship, and surveillance (Dick 2012). The internet is no longer a free and independent space, as it once seemed to be; it is now monitored and controlled to a large extent (Pariser 2011). Increasingly, countries, through their agencies and in collusion with major web companies such as Google, are restricting information flows, including access to potentially subversive information online (Maitland, Thomas & Tchouakeu 2012). The data from Google's transparency reports show, among other things, governments' requests for review of and/or removal of content from the web; some requests are granted, others are declined (Google 2012). Awareness and regular monitoring of trends on internet censorship in specific countries has become essential.

Papers by Bitso, Fourie and Bothma (2012), Dick, Oyieke and Bothma (2012) and Ekholm and Karhula (2012) – written as part of the Finnish Project on internet censorship and control on behalf of the International Federation of Library Associations and Institutions committee for Freedom of Access to Information and Freedom of Expression (IFLA FAIFE) – revealed internet censorship trends and set the scene for their regular monitoring. Two of these papers (Bitso, Fourie &

1. Constance Bitso is a Lecturer in the Library and Information Studies Centre, University of Cape Town, South Africa.

Bothma 2012, Ekholm & Karhula 2012) consequently triggered this author's interest in investigating internet censorship in South Africa. Although these papers may be perceived as being subjective (given that IFLA FAIFE has a vested interest in revealing censorship as it advocates freedom of expression), considering increasing global internet censorship, internet users need to be aware of the existence, purpose and implementation of censorship, irrespective of its justification. Transparency is crucial, particularly for institutions advocating freedom of expression on the internet. Lack of transparency is one of the greatest concerns for people and institutions that advocate freedom of expression and civil liberties. Murdoch and Roberts (2013) point out that, even in established democracies, transparency in internet censorship has proven difficult.

The current literature on internet censorship highlights its existence and possible circumvention strategies. The intention is to raise awareness of internet censorship. In affirming this, Murdoch and Roberts (2013: 8) postulate that "once society admits that censorship exists, the debate will begin to focus on whether the proposed censorship is proportionate, who has jurisdiction when standards vary between countries, and what checks and balances should be put in place to achieve transparency". Clearly, more discourse and research have to be undertaken on internet censorship to raise awareness, and to persuade authorities to be more transparent, where appropriate, about their internet censorship strategies.

This article emanates from a paper by Bitso and Fourie (2013) that was presented at the ProLISSA (Progress in Library and Information Science Southern Africa) conference. It reported on a data-mining investigation on internet censorship in South Africa during the period 2004 to 2014. It adapted the negative and positive censorship trends by Bitso, Fourie and Bothma (2012, 2013) when investigating internet censorship in nine countries: Australia, Chile, China, Finland, Libya, Myanmar, Singapore, Turkey, and the United Kingdom. A summary of the trends used in this article is provided in Section 4. While the negative trends propagate internet censorship, the positive trends oppose it (Bitso, Fourie & Bothma 2012: 2). Although what may be regarded as negative in one society may well be perceived as positive in another, in the context of IFLA FAIFE and institutions such as Electronic Frontier Foundation, Freedom House, Index on Censorship, OpenNet Initiative and Reporters Without Borders, all of which advocate for freedom of expression and civil liberties, it is deemed appropriate to categorise trends as positive and negative in this manner. It was in this context that the investigation of internet censorship in South Africa was done to raise awareness thereof in South African society. The investigation originated after noticing increasing global censorship; noting the lack of studies on internet censorship in South Africa (besides a *Wikipedia* (2014) article on internet censorship in South Africa) and recognising an observation that "minimal attention is being paid in South Africa to internet censorship and yet over time the government has developed controls that have made internet censorship much more possible" (Duncan 2012a).

2 Conceptualisation of internet censorship

This section conceptualises the term "internet censorship"; it defines the terms "censorship" and "internet censorship"; and then reveals internet censorship employed by governments through policy and legislation, including the reasons for and implications of internet censorship on society.

2.1 Censorship

The Oxford English Dictionary (2014) defines "censorship" as a "a mental power or force which represses certain elements in the unconscious and prevents them from emerging into the conscious mind" and a "censor" (noun) as "an official in some countries whose duty is to inspect all books, journals, dramatic pieces, etc., before publication, to secure that they shall contain nothing immoral, heretical, or offensive to the government". In the literature, censorship is defined as the control of information and ideas circulated within a society (Global Internet Liberty Campaign 2003); "the suppression of words, images, or ideas that are 'offensive' happens whenever some people succeed in imposing their personal political or moral values on others" (American Civic Liberty Union 2006); and as "the change in the access status of material, made by a governing authority or its representatives. Such changes include: exclusion, restriction, removal, or age/grade level changes" (American Library Association, in Hawthorne 1997). In the context of this paper, censorship is interpreted as any interference with information such as control, manipulation, suppression, restriction or removal in various formats or contexts including transition from one source to another.

2.2 Internet censorship

With the introduction of the internet, different forms of censorship and different motivations for censorship have evolved. Terms that are used include e-censorship, cyber censorship, net censorship and internet censorship (Bitso, Fourie & Bothma 2012). According to the Internet Society (2012), internet regulation is restricting or controlling access to certain aspects or information such as censorship of data, and controlling aspects of the internet such as domain registration and IP address control. Internet censorship is the control or suppression of the publishing or accessing of information on the internet. Although censoring information on the internet may be more difficult compared to other forms of media, several techniques have been developed and are in use in societies such as China, Iran, and Syria (Leberknight et al. 2012). Internet censorship is implemented in various ways such as filtering messages of dissent, preventing the spread of independent information online, or blocking social media, for example, Twitter in Turkey (Leiva-Gomez 2014) and Facebook and YouTube in China (Kyle 2014). Baldino and Goold (2014: 30) remind us that the internet is not anonymous because every user has an Internet Protocol address that allows technology-savvy people to determine one's location. In addition, through the use of cookies, a history of websites visited can be tracked, thus allowing large numbers of internet users to be categorised.

2.3 Internet censorship by governments

Apart from parents, teachers and religious groups and their leaders enforcing censorship (Robotham & Shields 1982), governments use legal frameworks, regulations and policies at various levels to enforce internet censorship (Bitso, Fourie & Bothma 2012). As a result, even highly democratic countries now issue frequent censorship and user data requests to digital content providers (Dick 2012). According to Meserve and Pemstein (2012), government internet censorship occurs, in part, for political reasons. In addition, countries inhabited by firms that produce substantial intellectual property (IP), censor digital content more than those that are poor in intellectual property. Moreover, in some flawed democracies, internet censorship follows political cycles, with countries pursuing more removal of content as elections approach. Furthermore, while democracies request content removal more often than authoritarian regimes, their requests are more likely to meet local legal standards than those made by authoritarian regimes (Meserve & Pemstein 2012). On a regular basis, the Economist Intelligence Unit (2012) provides a democracy index that ranks 167 countries according to the categories of "full democracy", "flawed democracy", "hybrid regimes" and "authoritarian regimes". These terms are used in this paper on the basis of the Economist Intelligence Unit Democracy Index 2012 which has categorised South Africa as a "flawed democracy".

The internet began without laws or policies for regulating behaviour. This seemed appropriate considering its rationale to have an open global wealth of free information. This "openness" has posed some challenges to societal virtues. Consequently, governments and various institutions have demonstrated the need to regulate the internet through policies and laws (Lyu 2012). We see that "a number of states have introduced policies to block access to internet content and websites deemed illegal which are even situated outside their legal jurisdiction" (Akdeniz 2010). However, the concern is that blocking policies are not always subject to due process principles; decisions are not necessarily taken by the courts of law; and often administrative bodies or internet hotlines decide which content or website should be subject to blocking (Akdeniz 2010). As a result, the blocking action is questioned with regards to the fundamental right of freedom of expression.

2.4 Reasons for internet censorship

According to Warf (2011), there are multiple reasons for internet censorship. These include political repression of dissidents, human rights activists, or comments insulting to the state (as has happened in China, Iran and Myanmar, for example); religious controls to inhibit the dissemination of ideas deemed unorthodox (as found in many Arab states); protection of intellectual property including restrictions on illegally downloaded movies and music; cultural restrictions that exist as part of the oppression of sexual minorities or ethnic minorities (for example, the refusal to allow government websites in certain languages).

Governments that seek to impose censorship do so in the name of protecting public morality from pornography or gambling and, more recently, combating terrorism (Warf 2011). Other reasons include national security, social stability and combating "cyber anarchy" (Goldsmith 1998 as cited in Warf 2011), or to prevent crime (Katyal 2001 as cited in Warf 2011). The South African government's reasons for imposing internet censorship are: the protection of children, national security, and the protection of intellectual property (Duncan 2012a). However, the concern of South Africa's media is that "governments often abuse these reasons to legitimise an internet control agenda" (Duncan 2012a). Whilst there may be various ulterior commercial, political or religious goals behind new forms of censorship, there are also groups of citizens who want to use filtering, forced identification and surveillance cameras because of concerns for child protection and crime detection (Karhula 2011). Nonetheless, the most worrying part in the new forms of censorship is that they are often hidden from users (Karhula 2011). The increased intrusion into internet use, enabled by technology, originates with different value judgments made by countries about the importance of free expression, protection of minority interests and concern for societal cohesion (Bambauer 2009: 3).

2.5 Implications of internet censorship

Although there may be good reasons for certain acts of internet censorship, the implications of this censorship need to be noted. For example, filtering technologies put in place to prohibit access to pornography by children, have been known to make mistakes. They block constitutionally-protected speech, while still allowing so-called objectionable material to be viewed (Maycock 2011). According to Maycock (2011: 8), filtering mechanisms suffer the risk of over-blocking, that is, blocking access to sites that were not intended to be censored, and under-blocking, or creating "false negatives", that is, allowing access to sites that were intended to be prohibited (Murdoch & Anderson 2008). In other words, over-blocking occurs when the web sites that were not meant to be filtered are blocked whereas under-blocking occurs when targeted web sites are missed (Deibert et al. 2008, Dutton et al. 2011, Hunter 2000). Sometimes, over-blocking is an attempt to avoid criticism, but at other times it proves to be a mistake resulting from overzealous interpretations of rules (Murdoch & Roberts 2013). Information flow is then negatively affected, one of the serious drawbacks usually highlighted by groups opposing censorship. However, filters are useful in some parts of the internet such as email boxes – it is through the technology of filtering, rather than legal controls, that spam and malware are tackled (McIntyre & Scott 2007).

The internet is relatively low in cost, easy to use, and allows participation in public debate, therefore its censorship or filtering impacts on the emancipation and free flow of information as well as spreading of intelligent ideas (Warf 2011). The internet allows access to multiple sources of information, including films and images; it has facilitated a generalised growth in awareness of foreign ideas, products, and political norms (Leberknight et al. 2010: 6). The internet and civil

society have increasingly come to co-evolve, energising and shaping one another in time and space (Warf 2011). All these are adversely affected by internet censorship, especially when implemented without transparency.

3. Method of investigation

Data-mining, referred to as "knowledge discovery in databases, the process of discovering interesting and useful patterns and relationships in large volumes of data" (Clifton 2010), was used to trace reports that relate to positive and negative trends on internet censorship in South Africa, adapted from Bitso, Fourie and Bothma (2012, 2013), in order to raise awareness about internet censorship. In January-February 2013, reports of incidences pertaining to internet censorship were traced on major news websites such as *BBC News*, the *Guardian*, *CNN* and *SA Media Database* as well as expert monitoring sites such as *OpenNet Initiative*, *Reporters Without Borders*, and *Freedom House*. The phrases used for searching were "internet censorship", "internet filtering", and "cyber censorship" all coupled with the keyword "South Africa". The process was repeated in April 2014 to update the information. The reason for using these news and expert monitoring sites was based on the experience and insights gained while investigating internet censorship for the IFLA FAIFE papers referred to earlier. The negative and positive trends adapted from Bitso, Fourie and Bothma (2013: 182-185) are outlined in the outcomes section below.

4. Outcomes of the investigation

The outcome of investigating internet censorship in South Africa is presented as a consolidation of incidents noted for each trend articulated in 4.1 and 4.2 below, mainly to raise awareness about internet censorship in South Africa. South Africa is ranked first for internet freedom in Africa (Freedom House 2012) but scored 26 on a scale of 0-100, where 0 depicts most free and 100 least free (Freedom House 2013). Although South Africa's internet freedom is high compared to other African countries, it still has some flaws in terms of global standards. Furthermore, South Africa is ranked fifth in the top ten internet countries in Africa (Internet World Stats 2012). The rankings (by internet penetration rates) according to Internet World Stats (2012) are Nigeria (48.4%), Egypt (29.8%), Morocco (16.5%), Kenya (12%) and South Africa (8.5%). This means that there are other African countries with higher internet access and penetration compared to South Africa; yet South Africa has more internet freedom compared to these countries. Therefore, an investigation of internet censorship in these African countries too is warranted.

Freedom House (2013, 2012) reports a growing internet penetration in South Africa: 21% in 2011 and 41% in 2012. Internet penetration and internet access rates are important elements that may help in assessing the presence of implied internet censorship. According to Bitso, Fourie and Bothma (2012), implied internet censorship occurs in situations where people are limited in the use of the internet and its associated technologies (for example, the World Wide Web) due to reasons often associated with the digital divide: the lack of Information Communication Technology (ICT) infrastructure, lack of computers, and lack of information and digital skills. Therefore, low internet penetration and access rates imply a form of censorship. Warf (2011) observes that:

- Internet penetration rates refer to the proportion of the population with regular access to cyberspace at home, school, or work.
- Internet accessibility reflects, *inter alia*, the willingness of governments to allow or encourage their populations to log into cyberspace.

4.1 Negative internet censorship trends in South Africa

Of great concern in South Africa is that the current internet and media freedom status may be affected by the Protection of State Information Bill (2010) (commonly known as the Secrecy Bill) and the lesser known General Intelligence Laws Amendment Bill (2011), enacted in 2013 (Solomon 2012). Restrictions on media freedom in South Africa have been receiving much publicity, even though most of the attention has focussed on threats to print and broadcasting freedom (Duncan 2012a, Kamaldien 2012a). There is a need to monitor the impact of the General Intelligence Laws Amendment Act 2013 on internet censorship in South Africa.

4.1.1 Internet-related privacy

According to Bitso, Fourie and Bothma (2012), in many countries there is a nationwide monitoring of internet access and use, with governments sometimes calling on the support of search engines such as Google, internet café owners and internet service providers (ISPs). Actions include invasion of individual privacy, such as interception of emails. In South Africa, there are reports that private companies are "ring-fencing" the internet by creating firewalls so that users cannot access non-approved content. There are also reports that social media users' data are being mined to sell to advertisers, and that procedures to opt out of resulting contact lists are often not user-friendly (Duncan 2012b). Vermeulen (2013) reports the discovery on Telkom SA Network servers of FinFisher Command spyware appearing as though it is the Firefox internet browser. One could interpret this as Telkom's assistance to the government on internet censorship. Once again, this situation is not unique: South Africa is one of the many countries – others include Australia, Canada, Netherlands, United States and United Kingdom – that hosts Command spyware on its servers (Vermeulen 2013).

Another aspect noted in South Africa is in restrictions to content such as blocking of file sharing sites (Freedom House 2012). The extension of monitoring is also potentially possible through the enactment of the Regulation of Interception of Communication Act (RICA) (2002) and in terms of the inspectorate under the Electronic Communications

and Transactions Act (2002) (Berger 2011). RICA requires all customers with cell phone numbers on cellular networks in South Africa to register their details with their respective networks. Customers are required to furnish service providers with full names and addresses, a copy of identity documents and proof of residence (Cassim 2012, Virtual Private Network 2013). The Electronic Communications and Transactions Act (2002) is meant to provide for the facilitation and regulation of electronic communication in South Africa (Republic of South Africa 2002). Again, this situation is not unique to South Africa because even established democracies have passed legislation for internet censorship and surveillance.

4.1.2 Internet control, filtering and blocking of content

According to Ekholm and Karhula (2012), in the ubiquitous information environment, the control of users extends to the management of persons and objects. The basis for the control is created by comprehensive and more efficient data collection and management procedures which aim at reaching everyone and everywhere. Ubiquitous technologies provide tools to identify, track and monitor any given person or object including communications and activities. In South Africa, like in many other countries, ubiquitous control and monitoring is attributed to tracking devices for various items such as vehicles, animals and children, including cell phone communication as well as the use of surveillance cameras in places such as malls, stations, airports and streets. According to Karasaridis (2012), there are reports indicating that the South African government conducts surveillance of mobile phone conversations, short-message services and emails through the National Communications Centre (NCC), a government agency that houses interception facilities. Although most interceptions involve reasonable national security concerns, such as terrorism or assassination plots, the system allows the NCC to record South African citizens' conversations without a warrant to do so. The General Intelligence Laws Amendment Bill (2011), enacted in 2013, legalises the interception of any communication that emanates from outside the borders of South Africa, passes through South Africa, or ends in South Africa (Karasaridis 2012), including the interception of modern social networking site activity, such as that on Facebook and Twitter. An email from an address originating from a foreign company or simple communication via Facebook could potentially be an interceptable communication (Suliman 2012). General intelligence laws authorise state security agencies to intercept intelligence from foreign signals without a warrant. The South African NCC can be likened to agencies such as the Central Intelligence Agency (CIA) and Federal Bureau of Investigations (FBI) in the United States of America.

According to Dick, Oyieke and Bothma (2012), filtering and blocking of internet content are done in various ways such as ISP-level content filtering, or mandatory national web filtering, where governments persuade internet service providers to create a voluntary system of filtering and blocking. At other times, domain names and URLs are blocked by identifying and collecting online content for censoring, thus compelling ISPs to remove the content concerned (Dick, Oyieke & Bothma 2012). It is reported that in South Africa access to foreign websites Netflix, Twitter and websites about internet security are problematic due to government policy of blocking file sharing websites (Virtual Private Network 2013). In addition, the Google Transparency Report (2012) shows that the South African government requested Google to remove eleven items from the internet between January and June 2012; three of these items were actually removed through a court order. The reason given for the removal of the items was defamation.

4.1.3 Internet-related media being censored

Internationally, censoring of social media websites, broadcasting sites, chat groups, and internet telephony services (for example, Skype) also occurs. For instance, in China blogs, Facebook, Twitter and other sites are blocked by denial of service. Other countries, like Australia, block websites for gamers and those selling games to children younger than fifteen years of age. In Libya, during Gaddafi's regime, the Aljazeera news television channel was blocked (Bitso, Fourie & Bothma 2012).

Although there is media freedom in South Africa, the most significant setback to internet freedom occurred when the Film and Publications Board was given jurisdiction over internet content, despite the fact that ISPs also self-police internet content through a notice and take-down procedure run by the Internet Service Providers' Association of South Africa (ISPA) (Duncan 2012a). ISPA is a non-profit South African internet industry body whose membership comprises large, medium and small internet service and access providers in South Africa (ISPA 2013). It is governed by a code of conduct which states, among other things, that ISPA members must take reasonable steps to ensure that they do not offer paid content subscription services to minors without written permission from a parent or guardian. In addition, ISPA members must provide internet access to customers with information about procedures and software applications which can be used to assist in the control and monitoring of minors' access to internet content (ISPA 2013).

A controversial amendment was introduced to the Film and Publications Act (1996) requiring any publication, with the exception of a newspaper recognised by the Press Ombudsman's office, to be submitted for classification if it contains the following material: sexual violence which violates or shows disrespect for the right to human dignity of any person; degrades a person or constitutes incitement to cause harm; advocates propaganda for war; incites violence; or advocates hatred based on any identifiable group characteristic and that constitutes incitement to cause harm (Duncan 2012b).

4.1.4 Technologies to monitor and identify citizens using the internet to express their opinion and to exercise freedom of speech

Increasing internet censorship also targets the control of individuals as several countries require identification, licensing or registration from users on the internet (Palfrey 2010). In such countries, ISPs conduct complete monitoring and storing of users' activities on the internet such as e-mail messaging, online searching including updates, and interactions on social

media such as YouTube and Facebook (Ohm 2009). Practically, intermediaries and service providers can monitor, regulate and control users' connections, use of services and their contents (Kelly & Cook 2011).

Although reports of internet censorship by government as well as by the private sector, including ISPs, were found for South Africa (Duncan 2012b), such as an arrest in Eldorado Park (reported by Berger 2011), the current investigation has not yet established the technologies that are used to monitor and identify citizens using the internet in South Africa. Perhaps this will transpire at a later stage as the research continues. Nonetheless, it should be noted that in South Africa at the moment the concern is more about the legislation that is likely to interfere with internet freedom.

4.1.5 Criminalisation of legitimate expression on the internet

The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression remains concerned that legitimate online expression is being criminalised in contravention of many states' international human rights obligations, whether it is through the application of existing criminal laws to online expression or through the creation of new laws specifically designed to criminalise expression on the internet (La Rue 2011). While increasingly sophisticated technologies are used to control citizens, including criminalisation of legitimate expression, adoption of restrictive legislation to justify such measures has been deployed (Ekholm & Karhula 2012). Internationally, such criminalisation ranges from intimidation of online journalists, bloggers and individual political activists, as has happened in China, Libya and Myanmar, through to journalists and bloggers being arrested and detained ("Internet enemies" 2011).

According to Berger (2011), in South Africa, defamation is settled either through a civil case or the perpetrator apologising, or the offending content being removed from the internet as reported in Google's Transparency Report (2012). Berger (2011) reports an incident where an individual was arrested in Eldorado Park under the common-law offence of *crimen injuria* for allegedly insulting someone on Facebook. Those opposing internet censorship view this incident as setting a bad precedent as well as being a politically-motivated suppression of blogging (Berger 2011).

4.1.6 Acts, regulations and legislation regarding use of the internet and enforcement thereof for internet censorship

Censorship and data surveillance have become a globally accepted condition (Ekholm & Karhula 2012). In 2010, more than sixty countries censored the internet, and many countries have passed legislation that sets restrictions on citizens' and the media's freedom of expression ("Internet enemies" 2011).

The investigation of internet censorship in South Africa revealed that the greatest concern is about the legislation that is viewed as a threat to internet freedom. Internet censorship includes the following:

- Regulation of Interception of Communications and Provisions of Communication-Related Information Act 2002 (RICA), which requires ISPs to retain data from customers for an as-yet-undetermined period of time and makes any internet system that is unable to be monitored illegal (Freedom House 2012).
- Electronic Communications and Transactions Act (2002) which created a legion of cyber inspectors whose job it is to inspect and confiscate computers, determine whether individuals have met the relevant registration provisions, as well as search the internet for evidence of "criminal actions" (OpenNet Initiative 2007).
- Internet and Cell Phone Pornography Bill (2010) which suggests a new role for mobile service providers and ISPs. According to the Bill "any internet service provider or mobile phone service provider who distributes, or allows to be distributed, through the internet or through a mobile phone in the Republic of South Africa, any pornography, shall be guilty of an offence and liable, upon conviction, to a fine or imprisonment for a period not exceeding five years, or to both a fine and such imprisonment" (De Wal 2010).
- Protection of State Information Bill (2010), known as the Secrecy Bill, has been compared to apartheid-era secrecy legislation because, according to this Bill, the State will decide what information is confidential and what is not (Dick 2012). Journalists found guilty of infringement of this Bill could face twenty-five years imprisonment (Dick, Oyieke & Bothma 2012).
- Films and Publications Act (1996) and its amendment aiming to regulate access to contents by the population.

An incident in South Africa was reported where a Christian advocacy group, Justice Alliance of South Africa (JASA), authored a document titled *Internet and Cell Phone Pornography Bill*. They proposed to make it illegal for ISPs in South Africa to distribute or permit the distribution of pornography. The document was presented to the then Deputy Minister of Home Affairs, who then asked the Law Reform Commission whether a change in the law was possible. Soon afterwards, the Deputy Minister of Home Affairs called for the fast-tracking of new regulation that would compel ISPs to filter content provided to users to ensure it does not contain any pornography ("Porn ban on net…" 2010, "Internet censorship in South Africa" 2014)

A report by Prince (2007) describes how a South African political party leader, Patricia de Lille, called for regulation of mobile social network service Mxit and internet blogs after discovering slanderous information about a popular rugby player; De Lille's suggestion was viewed as an attempt at internet censorship (Prince 2007).

4.1.7 Support of internet censorship by computer and internet companies, search engines and ISPs

As indicated earlier, governments are often the perpetrators of internet censorship and often tend to force other agencies to support censorship. An example can be found in China where internet censorship is not only enforced by ISPs but also internet cafés. Enforcement is by order of the government (Bitso, Fourie & Bothma 2012).

Internet censorship in South Africa is also becoming a cause for concern as "privately-owned ISPs play a role too in censoring the internet" (Kamaldien 2012a). Although the report by Kamaldien (2012a) does not state who ISPs censor, citizens in South Africa are, however, warned of the need to become more vigilant about businesses that censor internet freedom in South Africa and not focus only on government restrictions (Duncan 2012b, Kamaldien 2012b).

4.1.8 Internet-related communication surveillance

According to Duncan (2012b), with the passing of the Regulation of Interception of Communications Act (2002), the South African government developed the capability to spy on internet users. In the case of content originating outside the country, they can do so without an interception direction, which creates space for wide-scale abuses of the government's extensive monitoring and surveillance capacity. It has also been reported that the government appointed cyber-inspectors who can inspect any website for evidence of cyber-crime (Duncan 2012b). This author could not find reports that this was actually being practised. This could, however, mean that the cyber-inspectors are working is such a way that is not easily detected.

4.2. Positive trends in internet censorship in South Africa

It is quite common in a democratic dispensation for society to show discontent in areas that concern them. Communities oppose internet censorship by reacting in various ways such as circumventing the blocking of the websites intended to be censored and mobilising people to take action against censorship through online petitions or through virtual demonstrations (Dick, Oyieke & Bothma 2012).

4.2.1 Reactions to internet censorship such as changes in groups, group dynamics, responses and actions of groups

Reporters Without Borders joined the South African National Editors' Forum (Sanef), the Media Institute of Southern Africa-South Africa (MISA-SA) and the Freedom of Expression Institute (FXI) to urge parliament to reject the Film and Publications Amendment Bill 2006 proposed by the government ("Parliament urged to…" 2006). Some of the reasons given were: (1) the Bill would compromise press freedom; (2) there would be too much subjection to screening and authorisation, given that institutions such as the Independent Communications Authority of South Africa (ICASA) and the Press Ombudsman already exist to screen and authorise films and publications before release; and (3) a lack of transparency in the way the Bill was drafted.

4.2.2 Circumvention of internet censorship

During the process of investigating internet censorship in South Africa, it was not established whether any technologies or circumvention software and tools are used in South Africa. This fact could be attributed to internet censorship still being minimal in South Africa, particularly when compared to authoritarian states such as China, Iran and South Korea, which are categorised as "enemies of the internet" by Reporters Without Borders. However, there have been recommendations for foreign internet users to use Virtual Private Network (VPN) for privacy on the internet when they are in South Africa because it is alleged that the government of South Africa has a policy of blocking file sharing websites (Virtual Private Network 2013).

4.2.3 Cyber actions against internet censorship

According to Dick, Oyieke and Bothma (2012), South Africa's controversial Protection of State Information Bill (2010) has been the target of social media protest. Four of the top ten trending topics on Twitter in 2010 related to this Bill. In November 2011, Facebook and Twitter changed their avatars to a simple black image to show support for "Black Tuesday" in sympathy with protests against the Protection of State Information Bill (2010) which were taking place outside the ANC's Johannesburg headquarters and outside Parliament in Cape Town.

Rising global censorship at various degrees led people to find ways to bypass the censorship (Bailey & Labovitz 2011). To help censored users gain open access to the internet, different systems and technologies have been designed and developed that are referred to as censorship circumvention tools (Houmansadr et al. 2012). Circumvention tools and strategies for stringent internet censorship such as the Great Firewall of China are covered by Deibert et al., (2008). However, a key component for any censorship-resistant system or circumvention technology is to ensure privacy by enabling users to communicate undetected in a censorship network (Leberknight et al. 2010: 6). Since internet censorship in South Africa does not seem as strong as in other countries such as China, Iran, Pakistan and Myanmar (Bitso, Fourie & Bothma 2012), there is less need for innovative ways of showing opposition to internet censorship. This is probably the reason why, during this investigation, no reports were found on the use of cyber demonstrations in South Africa.

Both the negative and positive trends on internet censorship that were found in South Africa were presented in sections 4.1 and 4.2 above. Internet censorship in South Africa is not unique as most of the trends established here also exist in various countries, including in well-established democracies. Nonetheless, a negative trend, even if it is global, will be regarded as such in the context of IFLA FAIFE. The South African government, like many others, is making efforts to

govern cyberspace and digital media to ensure safety and security. The greatest challenge facing South Africa is spam, malware and incidents of hacking South African government websites, including, on more than one occasion in 2013, the website of the police by actors outside South Africa (Freedom House 2013). In some instances, this problem remains unsolved. In such situations, to combat crime and to ensure safety and security, internet censorship becomes unavoidable.

5. Conclusion and recommendations

Limited internet access can be interpreted as implied censorship (Bitso, Fourie & Bothma 2012). Thus, implied censorship in South Africa will decrease as internet penetration and access increases. However, there are reports of serious concerns that the latest developments in legislation will increase internet censorship. Therefore, constant monitoring of internet censorship is essential in South Africa, particularly focusing on government and ISPs. South Africa's internet censorship is at a point that it needs to be monitored closely in view of proposed legislation such as the Protection of State Information Bill (2010) and Internet and Cell Phone Pornography Bill (2011), as well as increasing hacking of websites. The big question is: what measures can be taken to raise awareness of over-blocking and to support regular monitoring of internet censorship in South Africa but still maintain safety and security? The approach of investigating reports on negative and positive trends used here is not exhaustive and it may be improved and continued from time to time; for example, Bambauer (2009) proposes an alternative process-oriented framework to evaluate the legitimacy of internet filtering. This is an approach that draws upon scholarship in deliberative democracy, health care decision-making, labour and environmental law, and cyber law, and postulates that legitimate censorship is open, transparent about what is banned, effective yet narrowly targeted, and responsive to citizens' preferences (Bambauer 2009). To assess legitimacy of internet censorship, Bambauer's framework (2009) asks four questions:

- Is a country open about its internet censorship including why its information being restricted?
- Is the state transparent about what material it filters and what it leaves untouched?
- How accurate is the filtering system: how well does content actually gets blocked – and not over-blocked or under-blocked?
- To what degree can citizens participate in decision making about internet restrictions, such that censors are accountable?

Lately, there has been a trend of co-opting the internet infrastructure itself to affect large-scale censorship (Bailey & Labovitz 2011). Although, the degree or severity of internet censorship and its impact on society is hard to measure (De Lange 1997: 1), some frameworks such as the one by Bitso, Fourie and Bothma (2012) as well as by Leberknight et al. (2010) may clarify levels of internet censorship. According to Leberknight et al. (2010: 6), the criteria for determining the prevalence and degree of internet censorship in a country – one that may be considered for South Africa – include the following:

- Cost: both resource and opportunity cost, which directly impacts the availability of censors.
- Scope: the range of communication modes censored.
- Scale: the number of people and devices that can be simultaneously censored.
- Speed: the reaction time of censors.
- Granularity: the resolution at different levels, for example server, port, webpage and end user device.
- False negative: the accuracy of censors.
- False positive: too high a false positive rate depletes the censor resources.
- Circumventability: how easily the censors can be disabled.

Given the latest legislation developments in South Africa, together with the concerns regarding internet censorship in the country, one may have to consider the above frameworks to gain more insight into South Africa's internet censorship, as well as establishing the prevalence of internet censorship in other African countries.

References

"Internet censorship in South Africa". *Wikipedia*. 2014. [Online]. http://en.wikipedia.org/wiki/Internet_censorship_in_South_Africa (06 June 2014).

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

American Civic Liberty Union. Censorship. 2006. *What is censorship?* [Online]. http://www.aclu.org/free-speech/censorship (10 January 2013).

Bailey, M. and Labovitz, C. 2011. Censorship and co-option of the internet infrastructure. Technical report. CSE-TR-572-11. [Online]. http://nsrg.eecs.umich.edu/publications/CSE-TR-572-11.pdf (06 March 2012).

Baldino, D. and Goold, J. 2014. Iran and the emergence of information and communications technology: the evolution of revolution? *Australian Journal of International Affairs*, 68(1): 17-35. DOI: 10.1080/10357718.2013.840263.

Bambauer, D. E. 2009. Cybersieves. Brooklyn Law School Legal Studies Research Papers; no. 149. [Online]. http://ssrn.com/abstract=1143582 (4 January 2012).

Berger, G. 2011. *Freedom of the African internet*. [Online]. http://www.thoughtleader.co.za/guyberger/2011/05/02/freedom-of-the-african-Internet/ (25 January 2013).
Bitso, C. and Fourie, I. 2013. Trends in transition from classical censorship to internet censorship: the case of South Africa*. Progress in Library and Information Science in Southern Africa (ProLISSA) Conference*. 7-8 March 2013. Pretoria, South Africa.
Bitso, C., Fourie, I. and Bothma, T.J.D. 2013. Trends in transition from classical censorship to internet censorship: selected countries' overview. *Innovation*, 42: 166-199.
Bitso, C., Fourie, I. and Bothma, T.J.D. 2012. Trends in transition from classical censorship to internet censorship: selected countries' overview. *FAIFE Spotlight*. [Online]. http://www.ifla.org/files/assets/faife/publications/spotlights/1%20Bitso_Fourie_BothmaTrendsInTransiton.pdf (20 November 2012).
Cassim, F. 2012. Addressing the spectre of cyber terrorism: a comparative perspective. *Potchefstroom Electronic Law Journal*, (15)2. [Online]. http://www.saflii.org/za/journals/PER/2012/27.html (25 January 2013).
Clifton, C.2010. Data mining. In *Encyclopedia Britannica*. Chicago: Encyclopaedia Britannica. [Online]. http://www.britannica.com/EBchecked/topic/1056150/data-mining (05 July 2014).
De Lange, M. 1997. *The muzzled muse: literature and censorship in South Africa*. Amsterdam: John Benjamins.
De Wal, M. 2010. The pesky fundamentalists and internet censorship. *Daily Maverick*. 1 October. [Online]. http://dailymaverick.co.za/opinionista/2010-10-01-the-pesky-fundamentalists-and-Internet-censorship (28 January 2013).
Deibert, J. G., Palfrey, R., Rohozinski, R. and Zittrain, J. Eds. 2008. *Access denied: the practice and policy of global internet filtering*. Cambridge, MA: MIT Press.
Dick, A. 2012. Established democracies, internet censorship and the social media test. *Information Development*, 28(4): 259–260.
Dick, A., Oyieke, L.I. and Bothma, T.J D. 2012. Are established democracies less vulnerable to internet censorship than authoritarian regimes? The social media test. *FAIFE spotlight*. [Online] http://www.ifla.org/files/assets/faife/publications/spotlights/2%20FAIFE_Dick_Oyieke_Bothma.pdf (20 November 2012).
Duncan, J. 2012a. The turning point for internet freedom. *The South African Civil Society Information Service*. 12 June. [Online]. http://sacsis.org.za/site/article/1329 (07 February 2013).
Duncan, J. 2012b. South Africa: the turning point for internet freedom. *allAfrica.com*. 12 June. [Online]. http://allafrica.com/stories/201206130117.html (07 February 2013).
Dutton, W.H., Dopatka, A., Hills, M., Law, G. and Nash, V. 2011. *Freedom of connection, freedom of expression: the changing legal and regulatory ecology shaping the internet*. Paris: Unesco Publishing.
Economist. 2012. *Economist Intelligence Unit Democracy Index 2012*. [Online]. https://portoncv.gov.cv/dhub/porton.por_global.open_file?p_doc_id=1034 (07 February 2013).
Ekholm, K. and Karhula, O. 2012. Sleepwalking toward a control society? Ten must-know trends. *FAIFE spotlight*. [Online]. http://www.ifla.org/files/assets/faife/publications/spotlights/sleepwalking-ekholm-karhula.pdf (20 November 2012).
Epstein, Z. 2014. *The most important thing you'll see today: internet censorship world map*. [Online]. http://bgr.com/2014/02/20/internet-censorship-world-map/ (20 April 2014).
Films and Publications Act, No. 65 of 1996. 1996. [Online]. http://www.info.gov.za/view/DownloadFileAction?id=70901 (20 November 2012).
Freedom House. 2012. *South Africa freedom on the net 2012*. [Online]. http://www.freedomhouse.org/report/freedom-net/2012/south-africa (13 January 2013).
Freedom House. 2013. *South Africa freedom on the net 2013*. [Online]. http://www.freedomhouse.org/report/freedom-net/2013/south-africa (25 April 2014).
General Intelligence Laws Amendment Bill, No. B25 of 2011. 2011. [Online]. http://www.parliament.gov.za/live/commonrepository/Processed/20111201/385713_1.pdf (13 January 2013].
Global Internet Liberty Campaign. 2003. *What is Censorship?* [Online]. http://gilc.org/speech/osistudy/censorship/ (13 November 2012).
Google. 2012. *Transparency report: South Africa*. [Online]. https://www.google.com/transparencyreport/removals/government/ZA/ (20 January 2013).
Halliday, J. and Garside, J. 2011. Rioting leads to Cameron call for social media clampdown. *Guardian*. 11 August. [Online]. http://www.theguardian.com/uk/2011/aug/11/cameron-call-social-media-clampdown (20 January 2013).
Hawthorne, C. 1997. *Censorship on the internet and in education*. [Online]. http://courses.cs.vt.edu/cs3604/lib/Censorship/Hawthorne.notes.html (12 December 2012).
Houmansadr, A., Zhou, W., Caesar, M. and Borisov, N. 2012. *SWEET: serving the web by exploiting email tunnels*. [Online]. http://arxiv.org/pdf/1211.3191v2.pdf (4 December 2012).
Hunter, C.D. 2000. Internet filter effectiveness: testing over and under-inclusive blocking decisions of four popular filters. *Proceedings of the 10th Conference on computers, freedom and privacy: challenging the assumptions*. 4-7 April 2000. Toronto: ACM. 287-294. [Online]. http://dl.acm.org/citation.cfm?id=332302 (25 May 2012).
Internet and Cell Phone Pornography Bill. 2011. [Online]. http://www.docstoc.com/docs/69957781/internet-and-cell-phone-pornography-bill (20 January 2013).

Internet enemies. 2011. *Reporters Without Borders*. 12 March. [Online]. http://viewsdesk.com/wp-content/uploads/2011/03/Internet-Enemies_2011.pdf (25 January 2012).
Internet Service Providers' Association. 2013. *Membership*. [Online]. http://ispa.org.za/membership/ (18 January 2013).
Internet Society. 2012. *Internet regulation*. [Online]. http://www.internetsociety.org/regulation (20 January 2013).
Internet World Stats. 2012. *South Africa internet usage and marketing report*. [Online]. http://www.internetworldstats.com/stats1.htm (20 January 2013).
Kamaldien, Y. 2012a. SA's internet freedom in trouble. *Cape Times*. 19 September. [Online]. http://www.iol.co.za/capetimes/sa-s-Internet-freedom-in-trouble-1.1386369#.UKv1nqDHjIU (07 December 2012).
Kamaldien, Y. 2012b. Censorship! Internet freedom in SA under attack. *The Media*. 11 September. [Online] http://themediaonline.co.za/2012/09/Internet-is-the-least-free-of-all-the-media-in-south-africa/ (07 February 2012).
Karasaridis, A. 2012. Online censorship in 2012. *Mail & Guardian*. 28 November. [Online]. http://mg.co.za/article/2012-11-20-looking-back-on-2012-online-censorship (21 January 2013).
Karhula, P. 2011. Freedom to read? Getting a picture of the internet censorship. *Signum*. [Online] http://www.ojs.tsv.fi/index.php/signum/article/download/4397/4107 (4 February 2012).
Kelly, S. and Cook, S. 2011. New technologies, innovative repression: growing threats to internet freedom. In: *Freedom on the net 2011: a global assessment of internet and digital media*. Freedom House, Ed. [Online]. http://www.freedomhouse.org/sites/default/files/FOTN2011.pdf (07 December 2012).
Kyle, 2014. *Internet censorship and its reasons*. [Online]. http://studyinchina.universiablogs.net/2014/04/28/internet-censorship-and-its-reasons/ (30 April 2014).
La Rue, F. 2011. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression for the United Nations General Assembly Human Rights Council 16 May 2011*. [Online] http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (21 January 2013).
Leberknight, C.S., Mung Chiang, M., Poor, H.V. and Wong, F. A. 2012. *Taxonomy of internet censorship and anti-censorship*. [Online]. http://www.princeton.edu/~chiangm/anticensorship.pdf (12 December 2012).
Leiva-Gomez, M. 2014. *Internet censorship: how countries block their citizens from entering websites*. [Online]. http://www.maketecheasier.com/internet-censorship-block-citizens-from-websites/ (12 April 2014).
Lyu, H. 2012. Internet policy in Korea: a preliminary framework for assigning moral and legal responsibility to agents in internet activities. *Government Information Quarterly*, 29(3): 394-402.
Maitland, C.F., Thomas, H.F., and Tchouakeu, L.N. 2012. Internet censorship circumvention technology use in human rights organizations: an exploratory analysis. *Journal of Information Technology*, 27: 285-300.
Maycock, A. 2011. Issues and trends in intellectual freedom for teacher librarians: where we've come from and where we're heading. *Teacher Librarian*, 39(1): 8-12.
McIntyre, T.J. and Scott, C. 2007. *Internet filtering: rhetoric, legitimacy, accountability and responsibility*. [Online]. http://www.academia.edu/178102/Internet_Filtering_Rhetoric_Legitimacy_Accountability_and_Responsibility (12 May 2012).
Meserve, S.A. and Pemstein, D. 2012. *Google politics: the political determinants of internet censorship*. [Online]. http://www.danpemstein.com/files/google.pdf (25 August 2012).
Murdoch, S.J. and Roberts, H. 2013. Introduction. In *Internet censorship and control*. S.J. Murdoch and H. Roberts, Eds. [Online] https://cyber.law.harvard.edu/pubrelease/internet-control/ (14 April 2014).
Murdoch, S.J. and Anderson, R. 2008. Tools and technology of internet filtering. In: J. Deibert, et al., Eds. *Access denied: the practice and policy of global internet filtering*. Cambridge, MA: MIT Press. 57-72.
Ohm, P. 2009. The rise and fall of invasive ISP surveillance. *University of Illinois Law Review*. 5: 1417.
OpenNet Initiative. 2007. *Regional overview of Sub-Saharan Africa, 2006-2007*. [Online]. https://opennet.net/studies/SubSaharanAfrica2007 (21 January 2013).
"Censorship". *Oxford English Dictionary*. 2014. [Online] http://www.oed.com/view/Entry/29607?redirectedFrom=Censorship#eid (12 April 2014).
Palfrey, J. 2010. Four phases of internet regulation. *Social Research*, 77(3) [Online]. http://www.law.harvard.edu/faculty/faculty-workshops/palfrey.faculty.workshop.summer.2010.pdf (28 January 2012).
Pariser, E. 2011. *Filter bubble: what the internet is hiding from you*. London: Penguin.
Parliament urged to reject bill that would legalise censorship of broadcast and print media. 2006. *Reporters Without Borders*. 18 August. [Online] http://en.rsf.org/south-africa-parliament-urged-to-reject-bill-18-08-2006,18601.html (25 January 2012).
Porn ban on net and mobiles mulled by South Africa. 2010. *BBC News*. 28 May. [Online]. http://www.bbc.co.uk/news/10180937 (5 February 2013).
Prince, N. 2007. MxIt founder hits back at call by De Lille for blog censorship. *Cape Argus*. 24 May.
Protection of State Information Bill, No. B6 of 2010. 2010. [Online]. http://www.parliament.gov.za/live/commonrepository/Processed/20111123/384294_1.pdf (30 November 2011).
Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA), No. 70 of 2002. 2002. [Online] http://www.justice.gov.za/legislation/acts/2002-070.pdf (25 January 2013).
Republic of South Africa. 2002. *Government gazette,* 446(23708). [Online] http://www.dod.mil.za/documents/acts/ECT%20Act25of2002.pdf (20 February 2013).
Robotham, J. and Shields, G. 1982. *Freedom of access to library materials*. New York: Neal-Schuman Publishers.

Sarkozy to host key internet forum ahead of G8 summit. 2011. *BBC News*. 24 May. [Online]. http://www.bbc.co.uk/news/world-europe-13513958 (27 January 2013).
Solomon, M. 2012. *Freedom House, internet freedom and dataless dark Africa*. [Online]. http://journoactivist.com/tag/Internet-censorship/ (5 February 2013).
Suliman, T. 2012. *The General Intelligence Laws Amendment Bill: Big 'GILA' is watching*. [Online]. http://www.polity.org.za/article/the-general-intelligence-laws-amendment-bill-big-gila-is-watching-2012-03-21 (25 January 2013).
Vermeulen, J. 2013. *FinFisher spyware servers in South Africa*. [Online]. http://businesstech.co.za/news/general/37268/finfisher-spyware-servers-in-south-africa/ (7 May 2014).
Virtual Private Network, 2013. *South Africa VPN: a way to secure your internet usage*. [Online]. http://countriesvpn.com/south-africa-vpn/ (25 January 2013).
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.
Witschge, T. 2008. Examining online discourse in context: a mixed method approach. *Javnost: the Public*, 15(2): 75–92.