WHAT ISPS CAN DO ABOUT UNDESIRABLE CONTENT

By Paul Esselaar.

A paper commissioned by the Internet Service Providers' Association (ISPA)[1].

ISPA Contact Details

Name: Elaine Zinn
Telephone: +27.11.314.7751
Fax: 086.606.4066 /+27.11.678.2097
Address: P O Box 3423, Parklands, 2121, South Africa
Email: queries@ispa.org.za
Web site: http://www.ispa.org.za

[1] For more information on ISPA see http://www.ispa.org.za.

1 CONTENTS

2 INTRODUCTION

This paper is intended to assist both Internet Service Providers (ISPs) and the general public to assess whether undesirable content, which is available by means of the Internet, can be restricted, and if so, in what way.

It is important to begin by emphasising that the success of the Internet has been based on the free flow of information and any restriction on this flow should be viewed with caution. With approximately 15-30 billion web pages available and approximately 1 billion Internet users[2], any attempt to filter or block content is a mammoth task which needs to be evaluated carefully.

In this paper the first issue that is addressed is the stakeholders who hold the keys to the flow of information via the Internet. Only these stakeholders are in a technically feasible position to filter or block content. Thereafter we focus on the definition of what constitutes "undesirable" content and the degree of "undesirability" of that content. A crucial next step is to differentiate the concepts of content blocking and content filtering as they are substantially different and are often misnamed in the popular press. The next section considers the practical implications of "opt-out" and "opt-in" Internet connectivity, where end-users would be provided with the choice to either opt-in or opt-out to receive certain undesirable content (such as adult pornography). The crucial role of education with reference to the many dangers present on the Internet is considered as well as the mechanism of Take-Down notifications which is already present in South African law. Finally some recommendations are made as to whether content should be filtered and if so, the practical ways in which the various stakeholders would be able to assist in combating undesirable content.

While this paper focuses on South Africa, several references are made to international examples and trends as the global nature of the Internet provides us with valuable insights as to the effectiveness, cost and technical feasibility of the different methods of dealing with undesirable content. As will be seen below, the global nature of the Internet is particularly problematic from the perspective of jurisdiction over offences, since the vast majority of web sites and content creators are not located in South Africa.

3 EXECUTIVE SUMMARY

Blocking undesirable content is technically difficult and never completely successful[3]. In some cases, such as with Bluetooth-enabled cell phones, blocking undesirable content can only be technically effected by the end user. While the determination of undesirable content is relatively easy to determine at end-user level, the determination of what is considered "undesirable" for all its customers places the ISP or telecommunications provider in an unenviable position, since any restriction is bound to make a significant proportion of its customers unhappy. Moreover the cost and resources needed to properly determine undesirable content and keep that list up to date is unfeasible for all stakeholders aside from the end user.

---

[2] The Size of the Web, Pandia Search Engine News,(accessed 08 April 2008). http://www.pandia.com/sew/383-web-size.html

[3] Indeed the recent survey by the South African Film and Publications Board indicates as much when it states that, "...it is more than likely that, even with blocking and filtering software, a child will be confronted with objectionable materials, educational strategies to equip children with knowledge on how to deal with and respond to such materials should be the focus of strategies to protect children online". See Report On Internet Usage And The Exposure Of Pornography To Learners In South African Schools, Iyavar Chetty, Antoinette Basson, 2008, (accessed on 15 May 2008) at pg.55. http://www.fpb.gov.za/research/docs/report.pdf

Current examples of blocking content internationally have created a false perception that "content filtering" is successful at ISP level. This half-truth camouflages the reality that only content blocking rather than content filtering is utilised, and this in turn is only used to block a small list of web sites and is easily circumvented.

South Africa already has the necessary legislation required to prosecute those offences that present themselves by means of the Internet. A focus on a synergy between ISPs, Interception Centres, the South African Police and the Film and Publication Board would result in the ISP being able to avoid legal responsibility for blocking content incorrectly and ensure that its independent status is maintained, the privacy of its customers is respected and that freedom of speech is not unnecessarily curtailed.

All stakeholders in the Internet cycle have a responsibility to assist end users to protect their rights and to educate the end user on the way in which they can filter content on their side. The fact is that no filtering technology is completely successful and can create a false sense of security. In order to combat this, the end users need to be educated by the stakeholders as to the technical options available to filter content, and the ways in which undesirable content can be combated using existing legislative tools, such as Take-Down Notices and reporting crimes via child-abuse hotlines or to the police. The police already have the necessary tools to intercept communications by means of an Interception Direction, and so both they, and the Film and Publications Board, need to be empowered to be able to carry out their mandate and prosecute those who contravene the legislation.

Where the offender is outside of the jurisdiction of South Africa, various international tools, such as treaties, need to be developed to foster international cooperation. While it is possible to block this content temporarily by means of a Take-Down Notice provided to all ISPs[4], or by means of ISPS subscribing to a voluntary list of blocklisted[5] sites, it should be noted that it is technically simple to circumvent these protections and that blocking the source of the content – i.e. the content provider – is the only lasting solution.

4 STAKEHOLDERS

The main stakeholders in the delivery of data via the Internet are:

- South African Government
- Telecommunications Providers
- Internet Service Providers
- Content Providers
- Financial Institutions
- Public Services
- End Users

4.1 SOUTH AFRICAN GOVERNMENT

[4] Provided that the ISPs voluntarily agree to respect take-down notices.

[5] "Blocklist" refers to a list of web sites/pages that are blocked. This is sometimes also referred to as "blocklisting".

The South African government is primarily represented by the Independent Communications Authority of South Africa (ICASA) that is mandated[6] to manage telecommunications within South Africa. Relatively recent changes to the legislation empowering ICASA[7] have been the subject of much debate and uncertainty. ICASA is particularly important as it has the power to declare the SAT3 cable[8] - an optical fibre connection linking South Africa to several other African countries and ultimately to Europe (Portugal and Spain) - an essential facility. Although access to the SAT3 cable was restricted to the previously state-owned telecommunications monopoly, Telkom, in terms of an exclusivity agreement, access to the cable is apparently now open to other telecommunications providers[9]. There are several other optical fibre connections that are in the planning process, most notably SEACOM[10] and the Eastern Africa Submarine Cable System (EASSy) which plans to connect the East African countries by means of an optical fibre cable. Finally there is also satellite access to the Internet.

Another important stakeholder, particularly in the area of undesirable content, is the Film and Publications Board (FPB) [11] which regulates and restricts many of the types of undesirable content that will be discussed below. The FPB is responsible for categorising content in terms of age restrictions as well as restricting content that is illegal – such as child pornography.

A final stakeholder would be the Office for Interception Centres which is created by s33 of the awkwardly named Regulation Of Interception Of Communications And Provision Of Communication-Related Information Act No. 70 Of 2002 (RICA). This office co-ordinates Interception Centres which obtain information from ISPs in accordance with the provisions of RICA.

4.2 TELECOMMUNICATIONS PROVIDERS

Until recently South Africa has suffered for many years under the yoke of a monopoly telecommunications provider Telkom[12]. Fortunately another fixed line telecommunications provider, Neotel[13], has now entered the market. Telkom was the only South African shareholder[14] in the SAT3 cable and has, until very recently, been the state mandated monopoly player in the "last mile" copper connections between end users and the telecommunications companies.

---

[6] In terms of s192 of the South African Constitution of 1996.

[7] The Electronic Communications Act no 36 of 2005.

[8] For more information on the SAT3 cable see http://en.wikipedia.org/wiki/SAT-3/WASC_(cable_system).

[9] As of 01 November 2007. See South Africa opens up SAT-3 cable system, Michael Malakata , IDG News Service, (accessed on 15 April 2008). http://www.networkworld.com/news/2007/103107-south-africa-opens-up-sat-3.html. It should be noted that ICASA issued a policy directive (as opposed to regulations) which is not binding on Telkom. See further Neotel breaks free from Telkom, 10 April 2008, (accessed 15 April 2008) http://it-online.co.za/content/view/257911/142/

[10] See http://www.seacom.mu/. Neotel is responsible for the landing of the cable in South Africa.

[11] Created in terms of the Film and Publications Act no 65 of 1996.

[12] Telkom SA Limited - http://www.telkom.co.za.

[13] Neotel (Pty) Ltd – http://www.neotel.co.za.

[14] SAT-3/WASC_(cable_system), Wikipedia, (accessed 15 April 2008). http://en.wikipedia.org/wiki/SAT-3/WASC_(cable_system)

Other notable telecommunications providers include the three mobile telephony companies, Vodacom[15], MTN[16] and Cell-C[17], of which the largest in South Africa is Vodacom.

4.3 INTERNET SERVICE PROVIDERS

South Africa has a number of Internet Service Providers (ISPs) most of which are members of the Internet Services Providers Association (ISPA)[18]. Competition in the area of data provision – as opposed to backbone telecommunications – has been fierce and this market is a relatively mature market.

4.4 CONTENT PROVIDERS

There are several million content providers who upload content to the Internet. Content providers would include content published on web sites, but would also include content published by means of an email and any other communication standards that the Internet is able to carry.

4.5 FINANCIAL INSTITUTIONS

While financial institutions are not directly involved in the provision of data via the Internet, many types of undesirable content - such as gambling - need to be paid for. Any restriction placed on the financial institutions to transfer money to the other parties has proved to be a major hindrance to these types of activities[19].

4.6 PUBLIC SERVICES

There are several other stakeholders that can be loosely classed as "public services". These would include the Internet cafes, schools and libraries, although South Africa still has some way to go before Internet services are generally available in libraries.

4.7 END USERS

The most fundamental stakeholders in the Internet cycle are the end users – both private individuals and commercial entities. While private individuals are not that well represented[20], corporate clients have considerable power and are generally well represented when it comes to lobbying for legislative change. End users would also include children – a type of end user that South Africa is at pains to protect.

5 WHAT TYPE OF CONTENT IS UNDESIRABLE?

[15] Vodacom (Pty) Ltd – http://www.vodacom.co.za

[16] Mobile Telephone Networks (Pty) Ltd – http://www.mtn.co.za

[17] Cell-C (Pty) Ltd – www.cellc.co.za

[18] For a list of the 147 ISPA members see http://www.ispa.org.za/about/memberlist.shtml.

[19] See for example House Backs Crackdown on Gambling on Internet, Kate Philips, 12 July 2006, (accessed 16 April 2008), http://www.nytimes.com/2006/07/12/washington/12gamble.html?_r=2&oref=slogin&oref=slogin

[20] The Internet Society of South Africa (ISOC-ZA) is one of the few civil society organisations that cater for the individual in South Africa.

Since the Internet allows every conceivable type of information to be communicated, only the main types of information that are considered to be undesirable are listed below.

5.1 CHILD PORNOGRAPHY

Child pornography in South Africa is currently defined as:

"*any image, however created, or any description of a person, real or simulated, who is, or who is depicted or described as being, under the age of 18 years and (i) engaged in sexual conduct; (ii) participating in, or assisting another person to participate in, sexual conduct; or (iii) showing or describing the body, or parts of the body, of such a person in a manner or in circumstances which, within context, amounts to sexual exploitation, or in such a manner that it is capable of being used for the purposes of sexual exploitation*."[21]

Thus child pornography in South Africa would also include those images and descriptions that are wholly created using computer technology, as well as those images or descriptions where the actors are, in fact, above 18 years of age, but represent themselves to be below the age of 18 and are engaged in sexual conduct[22].

The definition of child pornography is clearly very broad. As will be seen below the act of restricting this content can be extremely difficult, especially if the party responsible for restricting the content is unsure as to whether the image or description could validly be defined as "child pornography"[23].

5.2 ADULT PORNOGRAPHY

Adult pornography can be more difficult to define. While many forms of adult pornography involve graphic sexual conduct [24], the classification of the pornographic material can become progressively more difficult to define as it becomes less "hard-core". Currently all films are required to be submitted to the FPB for classification before being released. The impending Film and Publications Amendment Bill will also require

[21] S1 of the Film and Publications Act no 65 of 1996. It should be noted that a new Film and Publications Amendment Bill intends to amend this definition to include images or descriptions that are "*made to appear, look like, represented*" to be child pornography. See http://www.pmg.org.za/files/docs/070607b27b-06_0.pdf for this Bill. (Accessed on 15 April 2008).

[22] For a spirited criticism of this definition and the proposed amendment to the definition see: Submission on Films and Publications Amendment Bill (B27-2006) by Mark Oppenheimer (accessed on 15 April 2008) who proposes that the doctrine of "do no harm" should preclude the state from sanctioning child pornography where no image or description related to an actual child – i.e. virtual child pornography. He argues that films such as Shakespeare's Romeo and Juliet (B. Luhrmann Director, 1996) would fall within this definition as Juliet was 13 years of age when she had sexual intercourse with Romeo.

[23] See note 19.

[24] "Sexual conduct" is defined in the Film and Publications Act 65 of 1996 as including: (i) male genitals in a state of arousal or stimulation; (ii) the undue display of genitals or of the anal region; (iii) masturbation; (iv) bestiality; (v) sexual intercourse, whether real or simulated, including anal sexual intercourse; (vi) sexual contact involving the direct or indirect fondling or touching of the intimate parts of a body, including the breasts, with or without any object; (vii) the penetration of a vagina or anus with any object; (viii) oral genital contact; or (ix) oral anal contact. It should be noted that the Film and Publication Amendment Bill would introduce a new concept of "explicit sexual conduct" which, it is submitted, would be closely related to adult "hard-core" pornography.

computer games to be submitted to the FPB before release. This same Bill initially attempted to introduce pre-publication classification for newspapers, but this was strongly opposed[25] on the grounds that this would amount to censorship, and an exemption for this type of media was eventually provided.

Unlike child pornography which is completely illegal, adult pornography (which is classified as X18) is legally available to adults in South Africa. Since both children and adults access the Internet, a burden is placed on the stakeholders to ensure that adult pornography is not available to children. In particular, it is a criminal offence for an adult to allow children to access material that, if it were to be classified, would be classified as X18[26]. The problem of restricting undesirable content is further complicated by the fact that several lesser classifications (such as PG13) should also be unavailable to children who do not exceed the minimum age stated. While there has been some success in ensuring that physical material deemed to be X18 is restricted from children[27] (such as magazines and DVDs) the same cannot be said of access to similar material on the Internet which is often freely available.

In a recent survey released by the Film and Publications Board it was found that 64% of teenagers surveyed had been exposed to pornographic images on the internet, while 81% admitted to seeing such images on friends' cell phones[28]. The same study regards the exposure of children to pornography as "emotionally and psychologically toxic"[29]. That said only 6% of a child's time on the Internet was used to access pornography compared to 78% of the child's time on the Internet was used to obtain information for school projects[30] leading the survey to indicate that, "The Internet is becoming central to the learning process" [31]. While this survey provides useful data in the South African context, it should be noted that an incredible 81% of those surveyed had a computer in their home[32] which in turn suggests that the survey simply cannot be an accurate reflection of the demographics of South Africa and is more likely to be a reflection of the views of a more affluent section of society.

5.3 COPYRIGHT INFRINGEMENT

In general, the most common type of copyright infringement[33] that occurs by means of the Internet, involves the copying of commercial music and films. The South African Federation Against Copyright Theft (SAFACT)

[25] By, for example, the South African National Editors Forum (SANEF). See their submissions to parliament at http://www.pmg.org.za/docs/2007/071016sanef.pdf (accessed on 15 April 2008).

[26] Currently this conduct is prohibited by s26 read with s24 of the Film and Publications Act no 65 of 1996. This will be replaced by S24(A) of the Film and Publications Amendment Bill.

[27] See Films and Publications Regulations (Adult Premises) 2001, GNR.163 of 23 February 2001.

[28] See Cells, net 'are porn ponces', News24, 13 May 2008, (accessed on 13 May 2008). http://www.news24.com/News24/South_Africa/News/0,,2-7-1442_2321644,00.html . It should be noted that the survey found that more South African children were accessing pornography by means of cell phones (88%) than by means of the Internet (64%).

[29] See the FPB survey at pg.8. (For more details see note 3).

[30] See the FPB survey at pg.33. (For more details see note 3).

[31] See the FPB survey at pg.38. (For more details see note 3).

[32] See the FPB survey at pg.30. (For more details see note 3).

[33] Copyright is protected in South Africa by the Copyright Act 98 of 1978.

reports that 441,628 illegally copied units were confiscated in 2006, the vast majority of which consisted of DVDs and Video Cassettes (VCR). SAFACT estimates that over 50% of all DVDs sold in South Africa in 2005 were pirated[34].

Globally the problem of copyright infringement is of great concern to music and film companies. A recent decision by a Belgian court[35] required that Scarlet[36], a Belgian ISP, implement content filtering mechanisms[37] in order to prevent copyright theft. This decision is currently been appealed, but stirred up great controversy globally[38]. Two of the arguments put forward by ISPs – which will be examined below - were that (a) they would infringing on their users right to privacy if they filter the content, and (b) they were mere conduits of information and could not be responsible for the content that was transferred.

5.4 HATE SPEECH/DEFAMATION

Hate speech[39] and defamation[40] are similar only insofar as they normally are presented on the Internet in a similar way. However the similarity stops at that point since hate speech is a crime (also known as crimen injuria) and defamation can only be dealt with in a civil action. The growth of the Internet and new forums - such as blogs - have resulted in it being remarkably easy to publish material that is globally available. This is, of course, the primary attraction of the Internet. However the line between protected free speech, which legitimately criticises another person or entity[41], defamation and hate speech can be hotly contested and often

[34] Piracy In South Africa, SAFACT web site, (accessed 15 April 2008). http://www.safact.co.za/piracy_facts.htm

[35] SCRL Societe Belge Des Auteurs v SA Scarlet (No. 04/8975/A) as decided in July 2007.

[36] Formerly known as Tiscali.

[37] Eleven possible mechanisms to filter the content were suggested by the expert appointed by the court which included the use of Audible Magic software which filters out illegally copied content. These mechanisms have been subject to much international criticism. For further information see ISP Told To Block File-Sharing In Landmark Case, Out-Law.com, (accessed 15 April 2008). http://www.out-law.com/page-8239

[38] See for example the reply by the Electronic Frontier Foundation's reply to a call for copyright filtering by the music industry at: Music Industry Pressures EU Politicians for Filtered Internet, Danny O'Brian, 07 December 2007, (accessed on 08 April 2008), http://www.eff.org/deeplinks/2007/12/music-industry-europe-filter-pressure .

[39] Hate speech is defined in the Film and Publication Amendment Bill as: "the advocacy of hatred based on any identifiable group characteristic and that constitutes incitement to cause harm". S16(2)(c) of the South African Constitution of 1996 restricts freedom of expression when the comment expresses the, "advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm." This addition to the Bill has been criticised as an attempt by the South African government to censor public comment. See What You Can And Can't Say In South Africa, Dene Smuts, (accessed 15 April 2008). http://www.da.org.za/da/Site/Eng/campaigns/DOCS/Censorship-DeneSmuts.doc

[40] A comment is defamatory if it would lower the reputation of an individual or entity amongst right thinking persons in the community. There are several defences to publishing defamatory material such as: truth and public benefit, fair comment, denial that the comment is defamatory, absence of intention etc. Defamation in South Africa applies to both the written and spoken word unlike the United Kingdom for example which separates them into libel (written) and slander (spoken).

[41] A typical example of this would be the web site http://www.telkomsucks.co.za which criticises the fixed line telecommunications company Telkom.

difficult to distinguish. Clearly any effort to restrict speech in this area should be carefully considered, in order not to infringe on the positive effect of free speech which has been consistently emphasised by South African courts[42].

5.5 GAMBLING

Gambling in South Africa is currently regulated[43] at both a national and provincial level[44]. While the legislation governing gambling from physical premises is fairly stable, the regulation of online gambling in South Africa is in flux at present. Online gambling is currently illegal in South Africa[45], although this is extremely likely to change as soon as the National Gambling Amendment Bill[46] is enacted.

Restricting online gambling is also an international problem. A recent French court ruled that the French government's monopoly on gambling was anti-competitive and other competitors must be allowed to provide online gambling services in France[47]. The United States has also been struggling with online gambling for several years and recently was ordered by the World Trade Organisation to open up its borders to international online gambling[48]. Interestingly the United States made a significant impact on online gambling when it enacted laws preventing credit card companies from transferring the necessary funds to the gambling companies[49].

5.6 TERRORISM

[42] In S v Mamabolo 2001 (3) SA 409 (CC) para [37], Kriegler J stated:

"Freedom of expression, especially when gauged in conjunction with its accompanying fundamental freedoms, is of the utmost importance in the kind of open and democratic society the Constitution has set as our aspirational norm. Having regard to our recent past of thought control, censorship and enforced conformity to governmental theories, freedom of expression – the free and open exchange of ideas – is no less important than it is in the United States of America. It could actually be contended with much force that the public interest in the open market-place of ideas is all the more important to us in this country because our democracy is not yet firmly established and must feel its way. Therefore we should be particularly astute to outlaw any form of thought-control, however respectably dressed."

[43] In terms of the National Gambling Act no 33 of 1996.

[44] The Eastern Cape Gambling and Betting Board (ECGBB) is an example of a provincial body organised to regulate gambling.

[45] Online gambling in SA illegal, Siyabonga Mkhwanazi, IOL Technology.co.za, 29 November 2006, (accessed 15 April 2008). http://www.ioltechnology.co.za/article_page.php?iArticleId=3567877

[46] As published in Government Gazette no. 29489 on the 18 December 2006.

[47] OUT-LAW Radio, Matthew Magee, 19 July 2007, (accessed on 15 April 2008). http://www.out-law.com/page-8319

[48] The dispute was initiated by the Caribbean island of Antigua and Barbuda. See United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services, World Trade Organisation. http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm

[49] See note 17.

There is little doubt that the issue of terrorism has risen in stature after the terrorist attacks in America on 11 September 2001. Several countries have amended their legislation to deal with the threat of terrorism, which includes the ability to intercept communications and to decode encryption[50]. In addition, Europe is in the process of criminalising the publishing of information on bomb-making[51]. South Africa has also updated its communications interception legislation[52], cryptography legislation[53] and anti-money laundering legislation[54] (amongst others) to achieve similar aims.

6 CONTENT FILTERING / BLOCKING

It is essential that the distinction between content blocking (also known as index filtering) and content filtering (also known as content analysis filtering) be made, in order to clarify the substantial technical difference between the two. Content blocking broadly refers to an absolute denial of the content to the end user. This is generally associated with a blocked URL or IP address. In contrast, content filtering attempts to allow unrestricted material through, while at the same time stopping restricted material from being transmitted. Thus, in theory, content filtering would allow all the non-sexual text and images through from an adult pornography site, while content blocking would simply prevent the user from seeing the site at all.

Most filtering software uses a combination of both methods in order to prevent restricted data reaching the end-user.

Before addressing the technical methods that can be used, it should be noted that the statistical effectiveness of content blocking and filtering varies according to the stage at which the blocking/filtering occurs. As will be seen below, content blocking/filtering is technically more effective at end user level than at ISP or telecommunications backbone level. For this reason the success or otherwise of these methods is only addressed in section 10 below.

6.1 CONTENT BLOCKING

Content blocking is a popular method of restricting content, as it is relatively simple to implement. Examples of this type of blocking can be seen in the United Kingdom which has introduced a “cleanfeed” product which blocks certain web sites at an ISP level. Content blocking is also used in most content filtering products, such as Dan’s Guardian. There are three ways to block content:

[50] The Patriot Act in the United States of America is the most famous example of this. See “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" (Public Law Pub.L. 107-56).

[51] As indicated by Europe’s Commissioner for Justice, Franco Frattini. See OUT-LAW Radio, Matthew Magee, 19 July 2007, (accessed on 15 April 2008). http://www.out-law.com/page-8319. See further EU justice ministers agree to toughen laws on terrorism http, Elaine Sciolino and Stephen Castle, 18 April 2008, International Herald Tribune (accessed 13 May 2008). http://www.iht.com/bin/printfriendly.php?id=12147862.

[52] Regulation Of Interception Of Communications And Provision Of Communication-Related Information Act No. 70 of 2002 (as amended).

[53] Cryptography regulations in Government Gazette no 28594 published in terms of s94 of the Electronic Communications and Transactions Act no 25 of 2002.

[54] Financial Intelligence Centre Act 38 of 2001. Note that this Act is due to be amended shortly.

1. **URL based restrictions** – This method blocks content from a pre-determined list of URLs, such as http://www.sex.com.

2. **IP address restrictions** – This method blocks content from a predetermined list of IP addresses (i.e. 32 bit numbers that identify points (normally individual computers) on the Internet).

3. **DNS blocklisting/poisoning** – This method (also known as DNS manipulation) stops the Domain Name System (DNS) from providing the correct IP address of the computer hosting the web site. Thus for example after typing the URL of http://www.google.com my Internet browser would not be directed by the Domain Name System to the correct IP of 74.125.19.99 but to another IP address.

6.2 CONTENT FILTERING

Content filtering was developed in response to the ineffectiveness of content blocking (as detailed more fully below). Content filtering uses artificial intelligence to analyse and assess the content of a web page and respond, by either providing or restricting access to the web page, or part of the web page. Several different methods are used to filter content, many of which are considered to be proprietary and not available to the general public, and they vary in effectiveness. As expected, these methods are very resource intensive, slow and costly to implement. As filtering software differs widely in terms of the amount of resources, speed and costs associated with the software, it is not easy to generalise about the impact of content filtering software.

6.2.1 SPAM FILTERING VS CONTENT FILTERING

It should be noted that content filtering of web sites is not in the same position as spam filtering (of email) and enjoys less success due to the following reasons:

1. Any delay due to spam filters is generally unnoticed as emails are not "real time" communications.

2. Spam filters employ "honey traps" – i.e. fake email addresses that are specifically designed to catch bulk unsolicited email and add the email to a blocklist.

3. The similarity of unsolicited email allows companies to write appropriate algorithms to identify similar bulk unsolicited email and block it.

4. Email headers (unseen information that is used to direct the email and identify its source) can also be accessed to identify spam.

In addition to the above there are several other spam filtering techniques which are not common to content filtering and which allow spam filtering to be relatively more effective than content filtering[55].

7 THE OPT-OUT/OPT-IN SYSTEM

7.1 TECHNICAL FEASIBILITY

The opt-out (all Internet access is censored unless you opt-out) or opt-in (all Internet access is uncensored unless you opt-in) model is often proposed as a method to provide content filtering/blocking to those who

[55] Anti-Spam Techniques (email), Wikipedia, (accessed on 15 April 2008), http://en.wikipedia.org/wiki/Stopping_e-mail_abuse

would want it. The recent FPB survey recommended that, "ISPs should be persuaded to apply filters to all content, with adult end-users given the option of requesting unfiltered access through reliable age verification and password systems" [56].

While the full technical impact of an opt-out/opt-in system can be debated, some initial factors should be considered.

1. The opt-out/in system would require additional resources on the part of the ISP to manage the opt-in/out requests.

2. All requests would have to be verified in some way to prevent unauthorised persons (such as the child) from changing to the uncensored Internet.

3. The need for traffic from a filtered address to take a different route from that of a non-filtered address will result in technical difficulties for the ISP – especially with regard to routing.

4. The need to have two systems running simultaneously would also be costly and require maintenance.

5. All data (whether censored or not) would need to be examined in order to establish whether or not it should be filtered – effectively slowing down all Internet traffic.

6. It would be difficult for the ISP to distinguish when the parent was using the Internet (uncensored) and when the child was using the Internet (censored). This of course is not a problem for end-user filters.

These factors, combined with the question of whether South Africans actually want a filtering system as discussed below are very material when considering whether this type of system should be mandated.

8 THE ROLE OF EDUCATION

Education is of fundamental importance in dealing with content on the Internet. The ability to think critically and be aware of the dangers that exist online should be taught at an early age, and several initiatives are already in place online to do just this[57]. ISPs are in a good position to assist in providing educational material on their web sites and should make their call centre staff aware of the dangers related to the Internet and the options available to an end-user to deal with these dangers (such as implementing content filtering software on their PC). The ability to report undesirable content – whether it be spam, child pornography or hate speech – should be facilitated by the ISP. A parallel can be drawn with the current lack of precedent related to criminal prosecutions for spam. This argues that the general South African public has not been properly educated that sending unsolicited commercial email in a way that contravenes s45 of the ECT Act is a criminal offence.

One of the most compelling arguments in favour of education is that technical solutions are simply not possible in several situations. Examples of when technology struggles to protect the public would include adults grooming children for sexual encounters via encrypted chat room communications and children sending each other naked pictures by means of Bluetooth-enabled cell phones. Although there appears to be a high incidence of awareness that the Internet can be dangerous amongst South African teenagers the current statistics suggest that South Africa has to better its efforts to educate children in the light of the fact that approximately only slightly more than half (53%) of the teenagers in the FPB survey said that teachers discuss

[56] See the FPB survey at pg.57. (For more details see note 3).

[57] For example see http://www.commonsense.org which teaches Internet safety.

Internet safety and usage[58]. That said the fact that 90% of the teenagers surveyed were aware that their personal information should not be provided to strangers suggests that many South African children have at least some level of awareness of the dangers of the Internet[59].

9 TAKE-DOWN NOTIFICATION

In order to limit their liability ISPs are required to remove any content which is named in a Take-Down Notice which complies with s77 of the ECT Act[60]. However the requirement to remove content as a result of a Take-Down Notice is reliant on the ISP being a member of a representative body which has been formally recognised by the South African Department of Communications ("DoC"). Even though the ECT Act was promulgated in 2002 the DoC has yet to recognise any representative body, paving the way for an ISP to be unable to avoid liability even in cases where it is clear that the ISP was a mere conduit as envisaged by chapter 11 of the ECT Act[61].

Nonetheless the Take-Down Notice is an extremely useful tool in the hands of concerned parties and organisations and ISPA members currently voluntarily abide by Take-Down Notices[62]. ISPs should provide a form containing the required elements which can be downloaded from their web sites[63]. Once again, the impact of education with reference to Take-Down Notices should not be underestimated. ISPs would also benefit from a close working relationship with the Film and Publications Board (FPB), and the FPB itself would be in a position to provide the ISP with the relevant Take-Down Notices when appropriate.

10 WHO SHOULD FILTER/BLOCK CONTENT?

10.1 GOVERNMENT/TELECOMMUNICATIONS PROVIDERS

[58] See the FPB survey at pg.24. (For more details see note 3).

[59] See the FPB survey at pg.30. (For more details see note 3).

[60] S77 of the Electronic Communications and Transactions Act no25 of 2002 provides that a Take-Down Notice:

"…of unlawful activity must be in writing, must be addressed by the complainant to the service provider or its designated agent and must include-

a. the full names and address of the complainant;
b. the written or electronic signature of the complainant;
c. identification of the right that has allegedly been infringed;
d. identification of the material or activity that is claimed to be the subject of unlawful activity;
e. the remedial action required to be taken by the service provider in respect of the complaint;
f. telephonic and electronic contact details, if any, of the complainant;
g. a statement that the complainant is acting in good faith;
1. a statement by the complainant that the information in the Take-Down notification is to his or her knowledge true and correct; and

(2) Any person who lodges a notification of unlawful activity with a service provider knowing that it materially misrepresents the facts is liable for damages for wrongful Take-Down.

(3) A service provider is not liable for wrongful Take-Down in response to a notification."

[61] This oversight on the part of the DoC should be rectified immediately.

[62] See clauses 22-27 of the ISPA code of conduct. (Accessed 07 July 2008) http://www.ispa.org.za/code/code_of_conduct.shtml

[63] It should be noted that ISPA already provides this on its web site. See http://www.ispa.org.za/code/index.shtml (Accessed 07 July 2008)

10.1.1 FEASIBLITY OF CONTENT BLOCKING/FILTERING

The feasibility of filtering and/or blocking content at an optical fibre cable level is susceptible to the same technical difficulties that confront ISPs as detailed in section 10.2.1. As a result it would be inadvisable for an optical fibre cable level content blocking/filtering system to be implemented.

This does not mean that government, and particularly the Film and Publications Board (FPB), does not have an important role to play in educating the general public, providing child pornography hotlines and providing ISPs with Take-Down Notices. While content filtering is inadvisable due to the factors listed below, there are several other tools available to government – including criminal prosecution for the dissemination of various content such as child pornography – that the government could actively pursue.

10.1.2 COST

The South African government is funded by South African taxpayers. Moreover it is in direct contact with the main bodies responsible for declaring content undesirable – the FPB and the police. The FPB reports directly to parliament and is partly funded by government and partly funded by monies collected from its classification duties. The FPB has indicated several times[64] that it is under-funded in its efforts to combat undesirable content. The South African police services have set up a cybercrime unit but this unit in turn also needs significant funds and capacity building to be able to address the threats that already exist.

10.1.3 LEGAL RAMIFICATIONS

There is no legal obligation on ISPs to actively monitor communications[65]. Indeed it is illegal for an ISP to actively intercept or monitor communications[66], except as provided for in the RICA. The FPB, on the other hand, actively monitors web sites and has a child pornography hotline with operators who investigate child pornography (both online and offline). It seems clear that the FPB and the South African Police have a better ability and position to monitor content and report offensive content than ISPs.

10.2 ISPS

10.2.1 FEASIBLITY OF CONTENT BLOCKING/FILTERING

The effectiveness of content blocking on its own is generally poor. On the positive side, content blocking is somewhat able to restrict inadvertent access to offensive sites – that is, where the end user had no desire to access a web page bearing child pornography, but was directed there by means of a hyperlink in an email, for example. While the success of this technology is far from perfect, it could be argued that South Africa already provides for the removal of content in the form of the Take-Down Notice[67]. This "content removal" should not

[64] See Policing of child porn sites 'too slack', Cape Argus, 14 April 2008, (accessed on 13 May 2008. http://www.iol.co.za/index.php?set_id=1&click_id=13&art_id=vn20080414120010663C126041. See also Note 71.

[65] S78(1)(b) of the Electronic Communications and Transactions Act no 25 of 2002.

[66] See s2 of the Regulation of Interception of Communications and Provision of Communication Related Information Act no.70 of 2002 ("RICA").

[67] See paragraph 9.

be seen in the same light as "content blocking" as the ISP that receives the Take-Down Notice has direct technical control of the content that is being objected to.

The negative side of content blocking is, unfortunately, substantial. The following are some of the difficulties associated with content blocking/filtering.

1. **Go-to list of prohibited sites** - The creation of a blocklist of prohibited sites has the unfortunate technical consequence of broadcasting all those web pages to anyone who wishes to access undesirable content[68]. This effectively creates a "go-to" list for paedophiles.

2. **Circumvention of blocklist using anonymiser technology** - The ability of the ISP or government to restrict access to specific web pages can be circumvented by the use of "anonymiser" web sites[69]. These web pages are designed to remove all traces of the web page that you ultimately want to see and could be likened to "framing" the target web page. They have been particularly popular in countries where freedom of speech is heavily restricted - such as the Republic of China. From the ISPs point of view, the end user is not accessing the blocked URL, but rather he is accessing the anonymiser web site URL, which in turn is not on the blocklist. From the end users point of view, he still gets to see the web site he wished to access, albeit with a different URL contained in his address bar. While it is possible to also block access to these sites[70], it should be noted that these sites are often motivated by the need to liberate citizens of restrictive regimes[71] to see uncensored material and are, as a result, street-wise about ways to avoid censorship[72]. Moreover, some South Africans have a legitimate desire for privacy and this desire should not be prevented simply because it is possible to use these web sites to access undesirable content.

3. **Circumvention of blocklist/filtering using encryption** - Content blocking and filtering at ISP level is utterly useless if a site has implemented encryption. Thus, for example, if https://www.sex.com implements encryption, then content blocking would be unable to restrict access to the web page as the address of the web page and its content are contained in the encrypted payload that is only seen by the end user. All online banking uses encryption and open-source encryption certificates are freely available, frequently used and cheap[73]. As it is the express (and often legitimate) intention of

[68] *Failures in a Hybrid Content Blocking System*, Richard Clayton, University of Cambridge, Computer Laboratory. Paper presented at the Workshop on Privacy Enhancing Technologies, Dubrovnik, Croatia, 30 May 2005 - 1 June 2005. http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf

[69] For an example of a free anonymiser web site see http://www.anonymouse.org. It should be noted that despite its claim to block anonymiser web sites, as of 08 April 2008 http://www.cleanfeed.co.uk considered this site to be "allowed".

[70] It should be noted that translator web sites would also have to be blocklisted.

[71] In fact the United States government itself has sponsored similar technology in order to bypass Iranian censorship. See *SmartFilter's Greatest Evils*, Seth Finkelstein, 16 Nov 2000 http://www.sethf.com/anticensorware/smartfilter/greatestevils.php

[72] Examples of these methods include changing the web site name, adopting aliases and redirecting traffic from other (non-blocklisted) web sites.

[73] For example an open-source SSL Certificate from the ISP Hetzner costs only R149.00 per year.

encryption to restrict access, it is impractical to require all web sites not to use encryption and, more seriously, it is impossible to control the use of encryption due to jurisdictional difficulties[74].

4. **Parents abdicating responsibility** - Another difficulty relates to the public expectations created when a blocklist is implemented. It is not unlikely that a parent who knows that an ISP has implemented content blocking, would assume that the ISP would be generally effective in blocking undesirable content – especially with regard to his/her children. This could result in an abdication of responsibility by the parent who would be genuinely surprised to discover that undesirable content could still be easily accessed by his children as the blocklist did not, for example, cover adult pornography.

5. **Censorship** - Another problem relates to the degree to which the content is blocked. As more content is blocked, the degree to which undesirable content is blocked, naturally increases. This, in turn, results in a greater number of "false positives [75]" which would limit the right to freedom of speech. Indeed several claims of censorship have already been levelled at proponents of content filtering[76].

10.2.1.1 COST

The cost of blocking content at the ISP stage can be broadly broken down into four sections.

1. **The cost of creating the list** - The cost of creating the list at the ISP stage is much higher than the creation of an end-user list, and would require serious resources. For example, if the conservative estimate of 15 billion web pages is assumed, then the classification of 0.1% of these would amount to 15 million pages. If a person were to be able to classify 100 pages per day, it would take 150 working days to complete – by which time this list would be outdated. The size of this task is already clear to the South African Film and Publication Board, who have indicated that they lack the resources to effectively monitor the problem[77].

2. **The cost of maintaining the list** – Once the list has been created it needs to be maintained and blocked pages need to be add/removed from the list on a continual basis. A parallel can be made with China which currently employs hundreds of censors in an effort to ensure that their list is not outdated.

3. **The cost of dealing with complaints** - Once the web page is blocked, the ISP/government would require the necessary infrastructure and staff to deal with complaints from both web site owners (content providers) and end-users, who feel that the content should be accessible. This cost is dramatically escalated if "undesirable" content is taken to include all the categories of undesirable content detailed above. Unlike end user content blocking software, which can be turned on and off by

[74] While South Africa does, in theory, require all cryptography providers who provide a cryptography product within South Africa to be registered, this regulation is blatantly flouted by the global encryption community who provide free access to encryption technology on web sites. For further information on this requirement see Note 51.

[75] A false positive occurs when content is blocked which should not have been blocked.

[76] For example see From child porn to China , in one Cleanfeed, Lilian Edwards, (accessed 08 April 2008), http://www.law.ed.ac.uk/ahrc/SCRIPT-ed/vol3-3/editorial.asp

[77] As indicated by Ms Ms Bopape-Dlomo of the Film and Publications Board at the parliamentary hearings of the Home Affairs Committee on 15 November 2005.

the end user concerned, ISP level content blocking can only be turned off once a complaint has been made, investigated, decided and acted upon.

4. **The cost of hardware** – Unlike content filtering, content blocking is not as massively resource or bandwidth hungry. This does not, of course, mean that content blocking will not require resources to enable the common network that ISPs would need to connect to, to access and (if appropriate) update the list. In contrast, content filtering is extremely resource hungry, and requires significant investment on the part of the ISP in order to be operational.

5. **The cost of the software** – The cost of the filtering software varies widely from open-source tools to commercial filtering software.

While certain steps can be taken to reduce the size and cost of this undertaking, such as classifying "undesirable" content as restrictively as possible[78] and forging relationships with like-minded organisations that publish similar lists[79], content filtering/blocking is still a significantly expensive exercise for ISPs, many of which are small and battling to cope with existing legislation. For example, RICA has already increased costs ofr ISPs by requiring that they have the resources to be able to intercept communications seamlessly and report it to the Interception Centre.

While it is difficult to predict the exact cost involved in implementing a solution, it is useful to note that the Australian regulator in 2004 estimated an initial cost of approximately R331 million and an annual fee of R242 million to implement an ISP side content filtering solution for all Australian ISPs[80].

10.2.1.2 SPEED

There appear to be differing opinions as to the effect that a content blocking system has on bandwidth speed[81]. These differences seem to stem mainly from incorrect comparisons, where for example, the speed of content filtering was compared to that of content blocking. The best estimates indicate[82] that a small whitelist of web site delays the speed of bandwidth by approximately 1-2 milliseconds. In contrast, a large blocklist would introduce a delay of approximately 10 milliseconds which could, in turn, be compounded to result in a

[78] Probably to the extent of only identifying child pornography.

[79] Such as the Internet Watch Foundation (http://www.iwf.org.uk) which already communicates to the South African Film and Publications Board.

[80] Review of the Operation of Schedule 5 of the Broadcasting Act of 1992, Australian Government Report of 2004, (Accessed on 15 April 2008). http://www.dbcde.gov.au/__data/assets/pdf_file/0012/10920/Online_Content_Review_Report.pdf. Note that a currency conversion from Australian Dollars to South African rand was performed on 18 April 2008 and that the cost did not include redundant systems.

[81] For example Australian Minister of Parliament Kim Beazley claimed that "technology to implement mandatory filtering by ISPs is feasible and won't slow the Internet down" (Labor's Plan To Protect Kids From Internet Pornography, 20 March 2006, (accessed on 15 April 2008) at http://www.alp.org.au/media/0306/msloo210.php) in contrast to a report by Ovum (Internet content filtering - A Report to DCITA, Ovum, 4 April 2003. http://www.dcita.gov.au/__data/assets/file/10915/Ovum_Report_-_Internet_content_filtering.rtf).

[82] Internet content filtering - A Report to DCITA, Ovum, 4 April 2003. http://www.dcita.gov.au/__data/assets/file/10915/Ovum_Report_-_Internet_content_filtering.rtf

cumulative delay that is far more substantial. While the delay experienced by users is relatively uniform until saturation of the hardware tasked with dealing with the blocklist, the delay progressively increases after saturation point has been reached. It should be noted that ISPs have claimed a reduction in speed varying between 18 and 78 percent depending on the filter and content type[83].

When it comes to the Internet, speed is generally considered in seconds or milliseconds. End users have a real expectation that information will be provided to them quickly and ISPs compete with each other to provide a speedier service. The introduction of a blocklist of sites introduces the possibility of misclassification of web pages due to classification error, classification disputes and the classification being outdated. While the size of the blocklist is still relatively small, these issues are unlikely to cause broad concern. However as the size of the blocklist increases, such incidents will become more frequent and irritation over inability to access a legitimate site will increase. End users are unlikely to be forgiving when they are unable to access a web page for days due to a classification error, and are also likely to be motivated to bypass the content blocking by using the techniques described above.

10.2.1.3 LEGAL RAMIFICATIONS

One of the fundamental principles underlying Internet Service Providers is that they simply act as a mere conduit and do not moderate or control the content that is provided by their content providers. This "mere conduit" status legally allows them to escape liability for any damage, provided that they have complied with chapter XI of the Electronic Communications and Transactions Act[84] (ECT Act). Unfortunately, as mentioned above, the DoC has yet to recognise any representative body and as such has exposed ISPs to unnecessary risk.

Once the DoC has recognised a representative body, as soon as the ISP monitors, or in some way actively controls the content that is provided, there is the real danger that it has compromised its right to immunity, and so both it and the content provider himself could be sued. This in turn could result in an ISP being held liable for content which it unsuccessfully attempted to restrict using content blocking/filtering techniques.

In addition s78 of the ECT Act provides that ISPs "do not have an obligation to monitor" and do not have to "actively seek facts or circumstances indicating an unlawful activity"[85]. This section was drafted with the intention of relieving ISPs of the clearly impossible task of policing its users. The imposition of mandatory content filtering/blocking at the ISP level would reintroduce precisely the difficulties that the ECT Act tried to avoid. In addition it should be noted that the cost of retaining browser history is prohibitive[86].

---

[83] *Education the Best Filter for Young Australians on the Internet*, NetAlert Ltd, Media Release, 21 March 2006. http://www.netalert.net.au/03004-Education-the-Best-Filter-for-Young-Australians-on-the-Internet.asp

[84] No 25 of 2002. This section requires, amongst other things, that the ISP belong to an organisation such as ISPA and that they have no actual knowledge of the offending content. Failure to comply with a Take-Down notification would result in this immunity from liability being suspended.

[85] S78(1)(b) of the Electronic Communications and Transactions Act no 25 of 2002.

[86] See Policing of child porn sites 'too slack', Cape Argus, 14 April 2008, (accessed on 13 May 2008. http://www.iol.co.za/index.php?set_id=1&click_id=13&art_id=vn20080414120010663C126041 where Conrad Minnaar, a senior systems administrator at ISP eNetworks, said it would be impossible to store all browser records as it would require a great deal of money to implement.

Another major consideration is the right to privacy as enshrined in s14 of the Constitution of the Republic of South Africa. While it is easy to state that access to all web sites should be monitored[87], this approach is extremely difficult to justify, as the intrusion into the privacy of individuals is, it is submitted, substantial and constitutionally unjustifiable[88]. This, in turn, could result in a "fishing" expedition, where the police would submit a list of web sites that contained, for example, terrorist activities and the ISP would be obliged to submit a list of all its users that accessed those web sites. Moreover this approach would also persecute those people who inadvertently and unintentionally accessed the illegal web sites[89]. It should be noted that it is quite possible for communications to be monitored if an Interception Direction is obtained in terms of s16 of RICA, which in turn obliges an ISP to send the communications to an Interception Centre. S16(5) of RICA provides guidelines for judges to establish whether the interception of these communications is justified and whether this is an appropriate mechanism to use to intercept communications, where, for example, the trafficking of child pornography is suspected.

Lastly, it should be noted that ISPs lack the expertise to correctly classify material and are more likely to misclassify the media type. This, in turn, heightens the chance that ISPs could be sued for the incorrect classification of content, such as, for example, incorrectly blocking the commercial web site of http://www.kalahari.net which could cause serious financial damage, even if the site were blocked for only a short period of time.

10.3 CONTENT PROVIDERS

Offensive content is provided by content providers. In a perfect world it would clearly be the responsibility of content providers to be held accountable for any content that they send or make accessible. To a degree this is possible, provided that the content provider is resident in South Africa. As so many millions of content providers are not located in South Africa, and are often very difficult to identify, it is impractical to expect that all content providers (including those outside of South Africa's borders) will respect South African legislation. While it is self-evident that other stakeholders are in a logistically more practical position to restrict undesirable content, it should be borne in mind that the offending content did, in almost all cases, not originate with them. While the recommendation by the FPB to persuade content providers to rate their web

[87] For example the head of the FPB's compliance division Dumisani Rorwana states, ""It is important to monitor what the public is viewing, especially if they are watching child pornographic sites". See Policing of child porn sites 'too slack', Cape Argus, 14 April 2008, (accessed on 13 May 2008. http://www.iol.co.za/index.php?set_id=1&click_id=13&art_id=vn20080414120010663C126041

[88] See for example the complaint submitted by the Canadian Privacy Commissioner objecting to the streaming of the Internet by some large telecommunications companies in Canada. Privacy watchdog investigates Internet giants, Sarah Schmidt, Canwest News Service, 12 May 2008, (accessed on 13 May 2008). http://www.nationalpost.com/news/canada/story.html?id=510272

[89] This problem is commonplace as indicated by a United Kingdom study which found that "38% have been exposed to pornography through "pop-ups" while doing something else, 36% accidentally found themselves on a pornographic website when looking for something else and 25% received pornographic junk mail by e-mail or instant messaging". Approximately 70% of learners in Cape Town also came across pornography in this way. (as reported on pg.14-15 of the Report On Internet Usage And The Exposure Of Pornography To Learners In South African Schools, Iyavar Chetty, Antoinette Basson, 2008, (accessed on 15 May 2008). http://www.fpb.gov.za/research/docs/report.pdf.

site should be welcomed[90], it remains a sad truth that too much content is provided by content providers outside of South African borders for this initiative to make any substantial impact.

10.4 FINANCIAL SERVICES

As the United States has discovered[91], financial institutions are in a good position to restrict payment for certain undesirable services. An attempt to restrict financial transfers to companies that produce undesirable content was recently proposed in the Film and Publications Amendment Bill, but it is uncertain whether this will be included in the final version of the Bill. Moreover this restriction has been traditionally connected with online gambling rather than child pornography.

10.5 PUBLIC SERVICES

Public services, such as schools, Internet Cafes and libraries, often provide access to the Internet for persons who would otherwise have no access to the Internet at all. While these places can usefully implement content filtering software on a PC level, care should be taken to ensure that the content filter is not overly exclusive. A recent report issued by the FPB has supported the initiative to implement content filtering at a school and library, level[92] and has recommended that, "A multi-stakeholder approach is proposed between parents, caregivers and teachers in an effort to combine their knowledge and skills in guiding children with regard to Internet usage". [93] However care should be taken not to force filters to be overly exclusive as similar efforts in public libraries in, for example, the United States have been declared illegal due to their unnecessary infringement on freedom of speech[94].

10.6 END USERS

10.6.1 DO SOUTH AFRICANS WANT INTERNET FILTERS?

While it is very difficult to anticipate the response that the South African public (including businesses) would have to an opt-in/out solution without conducting a comprehensive study, anecdotal evidence from ISPA members currently indicates that less than 1 in 1000 of their clients request further details about content filtering/blocking. In order to anticipate the response of the South African public it is helpful to compare findings from other countries.

In terms of an Australian study[95], Australian ISPs reported only about a 1-2% take up on Internet filtering software, and that when an ISP offered a free trial of filtering software to its subscribers, less than 10% took up

[90] See the FPB survey at pg.57. (For more details see note 3).

[91] See note 16.

[92] See the FPB survey at pg.4. (For more details see note 3).

[93] See the FPB survey at pg.53. (For more details see note 3).

[94] See Mainstream Loudoun v. Loudoun County Library, U.S. District Court, Eastern District of Virginia, Case No. 97-2049-A at http://www.techlawjournal.com/courts/loudon/81123op.htm. (Accessed 15 April 2008).

[95] *Internet content filtering - A Report to DCITA*, Ovum, 4 April 2003. (accessed on 15 April 2008), http://www.dcita.gov.au/__data/assets/file/10915/Ovum_Report_-_Internet_content_filtering.rtf

the trial, and only 2% were willing to pay for the service. Moreover an Australian survey conducted in 2007[96], found that 74.4% did not want a mandatory ISP filtering system imposed.

Lack of interest in filtering software in a household does not necessarily mean that the household is technically incapable of implementing a filtering solution. There are several households that do not have children and so have no need to protect them from adult related material on the Internet. There are also several households that have no wish to filter content (viewing this as censorship[97]) and/or feel that they have educated their children sufficiently so that filtering software is unnecessary.

10.6.2 TECHNICAL FEASIBLITY

There is little doubt that end user filtering is far more technically feasible than filtering content at an ISP or telecommunications backbone level. This is equally true where the end user is a business rather than an individual. The reasons for this are:

1. The use of the end user's PC to filter content means that the processing power needed to implement the filter is handled by that PC and does not affect other end users.

2. PC based filtering is able to react more quickly to threats and block anticipated threats.

3. Overbroad PC based filtering only affects the individual PC rather than the entire Internet community. The approach of "one-size-fits-all" which is necessarily imposed by ISP or telecommunications backbone filtering is far more likely to result in a conflict between those who wish to view, for example, adult pornography and those who do not. As indicated above it is very likely that most end users do not want filtering at all.

4. PC based filtering can be individually customised according to the end user needs. In this respect it should be noted that the majority of films that were classified by the FPB in 2004/5 were rated below X18.[98]

5. PC based filtering is able to block other types of communication mediums (such as chat rooms, Peer to Peer (P2P) communications and FTP) which would not be possible for ISPs.

6. PC based filtering allows parents and children to use the same computer, but permits parents to easily unblock content that only they should see.

7. The easiest access that children have to the Internet is at home[99].

---

[96] Media and Communications in Australian Families 2007 p. 28 http://www.acma.gov.au/WEB/STANDARD/1001/pc=PC_310893

[97] For example see From child porn to China , in one Cleanfeed, Lilian Edwards, (accessed 08 April 2008), http://www.law.ed.ac.uk/ahrc/SCRIPT-ed/vol3-3/editorial.asp

[98] In terms of the FPB's annual report for 2004/5 films were classified as follows: 11.48% of the titles were classified "A", 20.73% were classified "PG", 8.62% were classified "10", 14.01% were classified "13", 12.87% were classified "16", 7.43% were classified "18", 24.11% were classified "X18" (adult material, only to be distributed via registered and licensed sex shops), 0.75% were classified "M" category. See http://www.fpb.gov.za/annual_reports/annual_reports.asp.

[99] See the FPB survey at pg.33. (For more details see note 3).

8. End user filtering is much cheaper (and can be free) as compared to ISP or telecommunications based filtering.

10.6.3 COST

The cost of blocking content depends on the stage at which you choose to block it. If the content is blocked at end user level, the cost is relatively negligible for the end user, and there are several commercially available software products and some open-source products[100] that can achieve this aim. However, the cost of the software does not appear to be the primary factor influencing the use of Internet filters as it is uncertain whether end-users would wish to have a content filter implemented on their PC.

10.6.4 LEGAL RAMIFICATIONS

Section 24B(3) of the Film and Publications Amendment Bill[101] indicates that it is an offence for an adult not to take reasonable steps to protect a minor from having access to material that contains depictions, descriptions or scenes of sexual conduct. This type of scenario is possible, for example, where an adult has pornography on his computer and his child uses the same computer for school projects. Content filtering at ISP level would not be able to provide the adult with the restricted content while at the same time making the computer safe for the child to use. This duty is more properly placed on the parent's shoulders.

11 CONCLUSION

It is clear that the problem of dealing with undesirable content is a complex one, which is made difficult by the cost and capacity needed to identify undesirable content correctly and keep it up to date.

Rather than focus on the difficulties that exist when seeking to block undesirable content, it would appear to be more useful to look at the proposed solutions.

11.1 IDENTIFYING UNDESIRABLE CONTENT

It can be seen that the identification of undesirable content is best left to the FPB and the South African Courts. Neither the telecommunications providers nor the ISPs have the expertise or capacity to correctly identify undesirable content. Moreover, placing this burden on ISPs or telecommunications providers, introduces further costs that will escalate already overpriced bandwidth and could subject ISPs to legal liability in the event that content is incorrectly classified. ISPs and telecommunications providers can, however, assist the public to identify undesirable content (without classifying it themselves) and assist the public to contact the appropriate authorities using the correct procedure.

11.2 BLOCKING UNDESIRABLE CONTENT

ISPs should only be responsible for restricting content where that content has been classified by the FPB, or has been objected to by a member of the public who has provided the ISP with a Take-Down Notice, or has been ordered by a court. Any movement from the independent status that ISPs currently hold would potentially attract legal liability and negatively influence the reputation of ISPs, who are at pains to respect the

[100] See for example the open source filter of Dans Guardian at http://dansguardian.org/ and the Collaborative Internet Filtering (CIF) project which uses the community to "tag" undesirable sites and block them.

[101] See note 19.

privacy of their customers and their ability to express themselves freely. That said, ISPs need to develop systems to allow themselves to quickly and efficiently block content once the requisite Take-Down Notice has been provided by the public or the FPB. The stakeholder that is most effective in blocking undesirable content is the end user, and several cost–effective tools exist to allow the end user to put a content filtering system in place. ISPs and telecommunications providers can assist end users to put these systems in place but should not have to bear the cost of providing the necessary resources and software, as this would escalate the cost of bandwidth, slow Internet access, create a barrier to entry for new ISPs and force ISPs to be involved in non-core business activities. For the reasons detailed above it is clear that blocking content at ISP level has not been very successful internationally and should be approached with caution.

11.3 PROSECUTING UNDESIRABLE CONTENT PROVIDERS AND USERS

ISPs would suffer substantial commercial damage if they were seen to be colluding with the police to conduct "fishing" expeditions and this has proved to be true in other jurisdictions. ISPs are not competent to police the Internet and would be ill-advised to attempt to do so. Content that is undesirable is already pronounced illegal in terms of existing legislation such as the Film and Publications Act and the Gambling Act. Clearly the role of policing any crimes under existing legislation is the function of the police and the necessary statutorily created bodies, such as the Film and Publications Board. ISPs can, however, assist these bodies to prosecute these crimes and there appears to be an obvious synergy that ought to exist between the police, the Interception Centres and ISPs, provided that the procedures that are set out in the existing legislation are adhered to. To belabour a point, an ISP should resist removing or blocking content where an Interception Notice or a Take-Down Notice has not been provided, as there exists a real possibility that these mechanisms themselves could be abused.

11.4 FINAL THOUGHT

There can be no doubt that there is freely available content on the Internet that is morally questionable and even illegal. In extreme cases, such as in actual child abuse being captured electronically, this content is overtly harmful and society has a duty to prevent this from occurring. Being confronted with this type of emotionally charged material leads to a temptation to implement substantial mechanisms at telecommunication backbone or ISP level, to ensure that this will never, ever, occur again[102]. This temptation should be avoided, as this approach is a false solution, and can give rise to further harm. Specifically, it is technically very difficult to successfully identify undesirable material and effectively block it without negatively, and substantially, impacting on the free flow of ideas and speech. Any type of restriction on either the ability of individuals to express themselves or their privacy, should be carefully considered. As Krieler J in S v Mamabolo stated: "we should be particularly astute to outlaw any form of thought-control, however respectably dressed"[103]. This is particularly true at ISP level where the intended list of blocked sites is not fully transparent and so unable to be challenged by the public. Achieving the balance between the harm that can be caused by means of the Internet and the immense benefits that the Internet provides is a difficult task. Without the support of all stakeholders this balance is unlikely to be found leaving South Africa the poorer.

[102] Indeed it is difficult not to have that type of reaction when faced with some case studies as described in the Report On Internet Usage And The Exposure Of Pornography To Learners In South African Schools, Iyavar Chetty, Antoinette Basson, 2008, (accessed on 15 May 2008) at pg.9. http://www.fpb.gov.za/research/docs/report.pdf

[103] See note 40.

12 ABBREVIATIONS

- DNS - Domain Name System
- ECT Act – Electronic Communications and Transactions Act no 25 of 2002
- FPB – Film and Publications Board (of South Africa) - http://www.fpb.gov.za
- FTP – File Transfer Protocol
- ICASA – Independent Communications Authority of South Africa - http://www.icasa.org.za
- IP – Internet Protocol
- ISP – Internet Services Provider
- ISPA – Internet Services Providers' Association – http://www.ispa.org.za
- PC – Personal Computer
- RICA - Regulation Of Interception Of Communications And Provision Of Communication-Related Information Act No. 70 Of 2002
- URL – Uniform Resource Locator