civil society advocacy programme

LAWYERS FOR HUMAN RIGHTS

Protecting Minors from Harmful Content via Mobile Phones

Project Report
18 May 2007

Prepared for Lawyers for Human Rights Child Rights Project
and Civil Society Advocacy Programme

by

Lisa Thornton Inc
ATTORNEYS

This document was produced for the Civil Society Advocacy Programme (CSAP SA 73200-03-03), a project funded by the European Union under the European Programme for Reconstruction and Development (EPRD), a partnership between the Commission on Gender Equality, the Office of the Public Protector, the South African Human Rights Commission and the European Union. The content of this document is the sole responsibility of its writer(s) and does neither reflect the views of the Civil Society Advocacy Programme (CSAP) nor the views of the European Union or any of the Public institutions taking part in this programme. For more information on CSAP and its programmes, please visit www.csap.co.za

Lawyers for Human Rights (LHR) and Civil Society Advocacy Programme (CSAP) embarked on this project in order to inform an advocacy project to bring about a balanced approach to the protection of children from accessing harmful content via mobile phones. The project report incorporates research with stakeholder input in order to formulate an overarching framework for promoting the protection of children and children's rights in the context of the stated concern.

Lisa Thornton Inc (LTI) was engaged to produce a background paper providing baseline data outlining the legal and situational analysis related to the cell phone industry and the protection of children. The situational analysis expounds on the uptake and usage of the technology and the types of content and concerns. The legal analysis provides the current legal and regulatory framework applicable to the concern.

The background paper served as a discussion document for the focus group which took place on 29 March 2007. LTI was engaged to produce a project report incorporating the input from the focus group discussion, and chart the way forward for Lawyers for Human Rights (LHR) and their partners. The project report concludes with a strategic plan on how LHR can contribute to the development of a policy framework promoting the protection of children from harmful content conveyed via mobile phones.

The legal and regulatory framework is attached as Annexure A. A list of the focus group participants is attached as Annexure B. During the focus group, a presentation by the Wireless Application Service Providers Association (WASPA) provided insight into some current self-regulatory measures in place. Youth Dynamix presented research conducted in respect of the use of mobile technology amongst the youth. A presentation by Childline put forward some of the psychological and emotional impact of child pornography and the use of technology upon children. (Copies of the presentations can be made available on request)

Included in this project report is background information on, amongst other things, the mobile communications market structure, penetration and usage, and our identification of potential concerns. Section 3 discusses the issues raised in the focus group and

section 4 looks at some strategies that could be implemented in South Africa as a result. In conclusion, we chart a course for LHR to embark upon.

1 Background Information

This section will provide an overview of what cell phone users can access on their telephones i.e. content, who the players in the mobile telecommunications market are, and how the technology supports the newer uses of mobile phones.

1.1 Sources of Mobile Communications Content

Generally, there are four sources of content that can be distinguished namely -

- Content provided by mobile communications operators i.e. the mobile phone companies and their resellers
- Content provided by third parties for a fee, the third parties are sometimes known as wireless application service providers (WASPs)
- Content available on the Internet, accessed via Internet Service Providers (ISPs)
- Consumer generated content, such as photos, video and SMS.

1.2 Mobile Communications Market Structure

In South Africa, there currently are three mobile communications operators, officially known as mobile cellular telecommunication services (MCTS) licensees (henceforth 'mobile operators') in terms of the communications regulatory legislation. The licensees are Vodacom, Mobile Telephone Networks (MTN), and Cell C.

Each of the mobile operators may exercise its rights through agents or service providers. Each of the mobile operators has entered into contracts with service providers, mainly for the resell of services to end user customers, for example Virgin Mobile South Africa and Nashua Mobile. Resellers are contractually engaged to sell the services offered by the mobile operators.

Similarly, wireless application services providers (WASPs) enter into contracts with the mobile operators so that they may provide content, usually fee based, to end user consumers via their mobile communications devices. Such WASPs include Exact Mobile and Clickatell. The content that may be sold varies from weather and sport

updates, to ringtones and screensavers, to adult material including photographs and video clips.

In addition to the service providers, the handset suppliers and manufacturers play an important role in the market structure. The handset manufacturers active in South Africa include Nokia, Samsung, Motorola, LG, Sony Ericsson, and Siemens.

For the sake of completeness, it is important to note that Internet access providers such as ISPs are licensed as value added network services (Vans) providers in terms of the relevant communications regulation legislation. This regulatory model, which applies to service providers such as ISPs and mobile operators, requires licensing in terms of an Act of Parliament. The licensing process is administered by the Independent Communications Authority of South Africa (Icasa), the regulator.

Providers of Internet content such as the WASPs, on the other hand, are not licensed and are not subject to regulation under the relevant communications regulatory legislation.

1.3 Newer Generation Mobile Communications

The original MCTS networks built in South Africa are what are commonly referred to as second generation or 2G networks. These networks mainly support voice services. Peer-to-peer SMS is commonly used on these networks as well.

The mobile operators in South Africa are beginning to build out 2.5G and 3G networks. These more technologically advanced networks will support more advanced services, such as access to the Internet and MMS. In addition, the speed and quality of service will be increased. Convergence – defined in this context as the provision of any service over any network – and the adoption of the Electronic Communications Act (discussed below) will lead to greater and more diverse content being available over mobile communications devices.

While mobile communications devices are currently used in South Africa by children mainly for SMSing and receiving voice calls, increasingly, they will be used for –

- MMSing
- SMS chatting

- Downloading logos
- Accessing all kinds of content
- As a payment method
- Accessing the Internet
- Audio and video streaming
- Gambling
- Gaming
- As a location device

Youth Dynamix, a commercial, research enterprise focusing on consumer behaviour amongst the youth, conducted a research study (BratTrax 2005) to track buying behaviour, product and media usage and lifestyle patterns within living standard measure (LSM), racial, age and gender groups. The study investigated various elements of the aforementioned including a variety of consumer goods, media, technology and telecommunications.

The sample consisted of 1110 respondents; 900 children and 210 moms, the children's ages varied between 7-15 years. All the subjects came from urban areas, but different socio-economic backgrounds.

The study recorded amongst others things

- a very high increase in cell phone ownership among all age groups from 2003 – 2005
- Large difference in cell phone ownership among income groups
- All age groups recorded a high usage of SMS, with voice services and game playing increasing
- Low usage of MMS and cameras
- Children of all ages aspire to the have the newest model of handset, illustrated by the instance of hand-me-down phones decreasing across the board
- Children mostly download ringtones, logos, games and 64% of moms are unaware of the frequency of use of premium rated services

2 The Concerns

Several media reports have appeared in the South African media relating to the issue of children accessing harmful content via mobile phones, causing concern to parents and

raising some alarm in schools. Despite this, research has shown that parents are rather positive about their children having access to mobile phones. The Youth Dynamix report indicates that 59 percent of parents indicate a very positive attitude and 35 percent report a quite positive attitude.

Hereunder we attempt to define the potential concerns. We draw a distinction between illegal content and harmful content. Illegal content is criminalised by the Films and Publication Act (FP Act) and offenders may be prosecuted. Harmful content, on the other hand, is not illegal; therefore purveyors of this type of content cannot be prosecuted under existing laws However, the content still causes harm therefore children's access to it must be limited.

2.1 Illegal Content

Two categories of content can be identified as illegal in South Africa, namely child pornography and hate speech.

2.1.1 Child Pornography

With respect to child pornography, a person is guilty of an offence if he/she possesses, creates or produces it, imports, procures, obtains or accesses it, or exports, broadcast or distributes it. Child pornography, according to the definitions in the Films and Publications Act (FP Act) is –

> 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 –
> (a) engaged in sexual conduct;
> (b) participating in, or assisting another person to participate in, sexual conduct; or
> (c) showing or describing the body, or parts of the body, of such person in a manner or in circumstances which, within context, amounts to sexual exploitation, or in such manner that it is capable of being used for the purposes of sexual exploitation.

Sending images via electronic communications networks, including mobile networks, which fit the description of child pornography, is a punishable offence. Detection is the main problem. The private and increasingly ubiquitous nature of mobile communications, due to, amongst other things, low costs, makes this issue a concern.

According to the Childline presentation at the focus group, children's exposure to and participation in child pornography causes the early sexualisation of the child and could cause severe psycho-social trauma such as emotional deprivation and other complex feelings related to post traumatic stress disorder. These feelings could range from anxiety to explosive or inhibited anger to full blown psychosis. It was pointed out during the presentation that there is a lack of research with respect to the harmful effects on children who view adult pornography. The presenter extrapolated the effects on children who viewed child pornography or were exploited during its making.

2.1.2 Hate Speech

Hate speech is illegal in South Africa. Although section 16(1) of the Constitution protects the right to freedom of expression, section 16(2) states that this protection does not extend to advocacy of hatred that is based on race, ethnicity, gender or religion, or that results in incitement to cause harm. In terms of section 29 of the FP Act, any person who distributes or shows a film, distributes a publication or presents entertainment or a play which, judged within the context -

(a) amounts to propaganda for war;
(b) incites to imminent violence; or
(c) advocates hatred that is based on race, ethnicity, gender or religion, and which constitutes incitement to cause harm,

shall be guilty of an offence.

Publication means –

(a) any newspaper, book, periodical, pamphlet, poster or other printed matter;
(b) any writing or typescript which has in any manner been duplicated;
(c) any drawing, picture illustration or painting;
(d) any print, photograph, engraving or lithograph;
(e) any record, magnetic tape, soundtrack, except a soundtrack associated with a film, or any other object in or on which sound has been recorded for reproduction;
(f) computer software which is not a film;
(g) the cover or packaging of a film
(h) any figure, carving, statue or model; and
(i) any message or communication, including a visual presentation, placed on any distributed network, but not confined to, the Internet.

2.2 Harmful (but not necessarily illegal) Content

Harmful content is not limited to illegal content. Hereunder we look at several categories of harmful content that are of concern.

2.2.1 Adult Content

Adult content, i.e. pornography and violence, is not illegal. However, it is considered harmful for children in a number of contexts. We live in an increasingly violent and sexualised society, as portrayed by the media. Statistics bear out the contention that media shapes our society, and the media has violent and sexual content.

The following statistics were provided by Lynne Cawood of Childline during her presentation -

- 42% of boys and 43% of girls report forced sex before 18 years
- 1/4 of women at Chris Hani Baragwanath Hospital report transactional sex
- 1/3 girls reported as having teenage pregnancy (Stats SA)
- Young persons are in high risk category for HIV/Aids
- 70% of children stumble across porn sites (KFF)
- Sex is the no. 1 searched for topic on the Internet (thumb.com)
- 20 000 child pornographic images posted on the net every week (thumb.com)
- 9 out of 10 children aged 8-16 viewed porn on the net (London School of Economics)

The regulation of children's access to harmful content is dealt with in a number of ways in traditional media, for example, by the age restrictions placed on films and publications. Amendments are currently being proposed to the F and P Act to bring the content of mobile media under the purview of the act.

The objective of the F and P Act is, in addition to criminalising child pornography, to regulate the creation, possession, exhibition and distribution of certain publications by means of classification, the imposition of age restrictions with due regard being had to the protection of children against sexual exploitation or degradation in any media.

A publication’s or film's classification determines how it may be exhibited, advertised, and distributed. Conduct contrary to a classification is a criminal offence and liable to prosecution.

Film means -

> (a) any sequence of visual images recorded on any substance, whether a film, magnetic tape, disc or any other material, in such a manner that by using such substance such images will be capable of being seen as a moving picture;
> (b) the soundtrack associated with and any exhibited illustration relating to a film as defined in paragraph (a);
> (c) any picture intended for exhibition through the medium of any mechanical, electronic or other device.

The definitions of publication and film make the ambit of the Act include any communication via an electronic communications network. As there is no other classification body, the FPB fulfils an important role. However, it is important to note that the board members are appointed by the Minister of Home Affairs, therefore the board cannot be said to be independent. Furthermore, the proposed amendment to the FP Act attempts to bring broadcasting under the purview of the act. This provision would be patently unconstitutional as section 192 of the Constitution provides that national legislation must provide for an independent authority to regulate broadcasting to be fairly representative of the diversity of South African society. That independent authority is Icasa. The classification function of the FBP can however, as proposed in the amendment bill, be extended to include interactive computer games and content accessible on mobile phones.

The legislative provisions with respect to the classification of adult content are repeated in the South African Cellular Operators Association Code of Good Practice (SA Cellular Code) as well as the Wireless Application Service Providers' Association Code of Conduct (WASPA). These are self-regulatory codes. They are more fully discussed below (Par 3.2.1).

2.2.2 Interactive Services and Location Information Services

Interactive services are of concern in relation to children because they provide a means for predatory individuals to lure children into face-to-face meetings, where they may be abused, abducted, or even killed. Interactive services include services such as chat rooms, also known as social networking services. Chat rooms operate by users creating online personalities or profiles who interact with each other. These services offer largely independent and unsupervised channels of self-expression for children and opportunities for them to interact with old friend and make new ones.

Unfortunately, these services also present these opportunities to individuals with ulterior motives. Sexual predators often create false profiles in chat rooms and engage in a behaviour known as ‘grooming’. Grooming happens when children are prepared for illicit, often sexual activities, by gaining their trust and often alienating them from their family and friends. It has been found that children often engage in more risky behaviour when using the chat rooms because it is not ’real’ and due to its anonymous nature. Therefore, children may talk about sex to a stranger online or disclose personal information, such as their address or the name of their school.

This concern is increased as location information services become available, potentially making it possible to find the location of children without their knowledge.

Although the ultimate insult - abuse, abduction, or murder – is an offence in South Africa, the concern of the industry should be to avoid making the means of such an offence available to offenders.

These crimes are not, however, the only harm that may befall users of interactive services. In part, due to the anonymity that cyberspace offers and the pervasiveness, mobile phones are rarely switched off, cyber-bullying and cyber-threats are also causes for concern. This form of bullying, much the same as traditional forms of bullying, can cause feelings of embarrassment, denigration, and low self-esteem in children, which could lead to suicide.

The monitoring of chat services might be one self-regulatory method whereby the industry could minimise the risk that children are exposed to when using interactive services. Another recommendation to the industry would be making all accounts/profiles private, so that they can only be accessed by persons specifically authorised by the account holder. By segregating sites, the industry can assist by prohibiting a twelve-year old from networking or interacting with a 21- or 31-year old. Violators of age-requirements could be punished by closing their accounts and informing parents in the case of minors.

It might also be possible to identify past offenders, denying them access to such services in future. This will require the cooperation of the prosecution authorities.

2.2.3 Unsolicited Communications (Spam)

Spam is currently a problem in respect of email and increasingly by SMS. The receipt of unwanted messages is not only annoying, it is a waste of time and resources for the receiver. A further concern is the receiving of illegal or harmful content, such as child pornography, hate speech or adult content, by children.

Spam is not new to mobile communications. The methods that have been employed to deal with it over time have proved successful to some extent. History has given us technological as well as self-regulatory methods in which to deal with spam. A combination of strategies will likely be necessary also in respect of mobile communications.

2.2.4 Premium Rate Services and other Commercial Transactions

Premium rates services have become payment methods, for information and other services. Often times, the payment amount, and even sometimes the method itself are non-transparent to the consumer. Children especially are susceptible to the lures of downloading ring tones, logos, games, music and other stuff and this is more often than not, done without the knowledge of the parent, who is paying for the service. Children are also particularly vulnerable to deceptive advertising practices and fraud.

Another danger is that children will hand out personal and confidential information such as credit card details. Further, applications for mobile communications devices will likely, in future, include usage for micro financial transactions, much as credit cards are now used.

Of special concern where children are concerned is the issue of gambling. Mobile operators that enable gambling by allowing their billing systems to be used for charging gambling debts, is not uncommon. Without effective means of verifying the age of the user, it will be difficult to prohibit this convenient and private method of gambling.

2.2.5 Peer – to – Peer Communications

Perhaps the most difficult concern is that of peer-to-peer communications. One example of peer-to-peer communications is file sharing such as that done over networks like Napster. In this respect, the issue of copyright protection (which is not fully canvassed/ addressed in this paper) is a concern.

Another aspect of peer-to-peer communication is the bullying or harassing of fellow children. Although the advent of mobile communications did not bring with it the age-old problem of bullying, the fact that mobile communications devices are always on, makes it a particularly invasive manner of bullying. It has been reported in the South African media that children take photos of one another in compromising activities, such as toileting and having sex, and then distribute those images via MMS. This type of bullying is reportedly more traumatic for the victim than more traditional forms of bullying, which are also common via mobile phones, such as threats and crank calls.

2.3 A Balancing Act

In plotting an appropriate response to children accessing harmful content via mobile phones, it is important to keep two principles in mind. First, the Constitutional right to free expression must be respected. Second, in our zeal to protect children we must not forget to promote the positive use of powerful technology. The many cultural, social and educational benefits that mobile technology offers children and any proposed solutions should work together to ensure that access and information rights are preserved to the greatest extent possible whilst balancing appropriate concerns. Children have a right to be protected, but they also have a right to be empowered.

3 Focus Group Report Back

All the participants at the focus group welcomed this initiative as a positive start to a useful debate. The focus group was useful in introducing various players to each other and familiarising the regulatory framework to stakeholders outside of the mobile communications industry. The majority of the main stakeholder groups were represented at the focus group. The industry was represented by the MCTS providers, content providers, and industry representative bodies. No equipment manufacturers were present. Civil society was well represented, primarily by child welfare

organisations. The government agencies represented were the Film and Publication Board (FPB), the Department of Communications and the ICASA.

The lack of representation by the prosecuting authorities and formal education agencies resulted in a discussion that possibly fell short in addressing or constructively engaging the concerns raised in an inclusive and holistic manner. As the prosecution of offenders is a key part of addressing any social problem we attempted, unsuccessfully, to get input from the prosecuting authorities on specific difficulties, successes and contributing factors in prosecuting and rehabilitating offenders. Due to the lack of input by formal education agencies, we were unable to establish whether banning cell phones in schools is a workable solution, amongst others. Other issues which were not fully canvassed are alternative strategies which may be employed in schools and, most notably, children's view of the perceived problem.

This section looks at the main issues that were raised by the focus group participants and by our research.

3.1 Research

One of the more significant issues revealed during our desktop study, was the lack of research available on the extent of the problem as stated. The European Commission (EC) engaged in a similar study and had to rely on research available with respect to Internet usage by children. In order to properly situate the concerns in context, the EC then engaged in a public consultation process in order to more accurately gauge the extent of the risks and responsibilities of the various players.

Due to the nature of the mobile device and the way in which it is used, it is possible that the problem is much more prevalent than is suggested by the lack of media coverage, alternatively, that there is no real problem at all. Therefore, it is imperative that more research is conducted before measures are implemented to curb children's access to the mobile technology, which can be used in many beneficial ways.

A form of technology in respect of which some research is available is Mxit, the chat application or message exchange service. Using Mxit is simple and cheap and it has taken South Africa's youth by storm. The statistics for usage of Mxit includes 120 000

000 messages per day. The age profile of users in April 2007 looked like this, according to Gillian Clapham, Business Development Manager, Mxit Lifestyle:

Age of user	Number of users
Up to 11 years	68 027
12 – 18 years	1 274 666
19 – 25 years	1 098 829
Above 25 years	584 356
No age given	727 751
TOTAL	**3 753 630**

In addition, there are approximately 7,000 – 11,000 new registered users per day.

Mxit, like other social networking sites has certain risks associated with its use. These are –

- Unsafe disclosure of personal information
- Addiction to the sites
- Risky sexual behaviour
- Cyber-bullying and Cyber threats
- Dangerous Communities

The numbers indicate that Mxit is, indeed, a technological revolution and a profound change in how a tenth of our population communicates. Anecdotal evidence suggests that addiction to Mxit is prevalent with adolescent girls. However, more research, especially into the emotional and psychological impact of the use of the technology, is needed to plot an appropriate response.

3.2 An appropriate regulatory response

All players in the mobile communications industry agree that they have a social responsibility, in particular in the area of access to commercial content which may be harmful or illegal. However, some of the concerns or possible risks lay outside of their responsibilities and capabilities, specifically the risk related to contact, namely bullying and grooming. A suitable regulatory framework is required to address this issue.

3.2.1 Self-regulation

There are three industry representative bodies (IRB) currently active in the mobile communications industry, namely the Internet Service Provider Association (ISPA), WASPA and South Africa's Cellular Operators Association. They were formed in terms of chapter XI of the Electronic Communications and Transactions Act (ECT Act). The ECT Act was enacted to provide legal certainty to the use of electronic communications and technology in commercial transactions. The relevant section of the Act provides for the limitation of liability of service providers if certain conditions are met, namely the adoption of an enforceable code of conduct and recognition of the IRB by the Minister of Communications (Minister). The IRBs have adopted codes of conduct, but have not obtained recognition from the Minister in terms of guidelines published by the Minister in Government Gazette 29474 on 14 December 2006.

WASPA is the IRB most relevant to the regulation of content accessed via mobile phones. In terms of the self-regulatory model adopted by Waspa, everyone, except members of WASPA is excluded from all of its processes. Any body, whether statutory or voluntary, that attempts to regulate a billion rand industry must have its processes open to public scrutiny and input.

The purpose of an IRB is, above all, to protect consumers and, in so doing, promote confidence in the industry. To be workable, however, it is necessary that codes of conduct adopted by IRBs be the product of genuine consultation between government and the industry, further strengthened by meaningful dialogue with non-governmental groups and the interested public. It is also important that the codes be understood by those who are limited by its provisions as well as those seeking its protection. The codes must also be backed up by clear lines of accountability and monitoring.

Self-regulation or the model that has been adopted by WASPA is not the panacea. What are required in this nascent and fast changing industry are transparent processes with broad-based involvement from all interested stakeholders. These requirements speak to a co-regulatory model, where some powers are retained by the industry, but government retains a measure of jurisdiction.

3.2.2 Co-regulation

Different models of co-regulation have been adopted in other jurisdictions with varying degrees of control and involvement by government. In Norway, for instance, Telenor

Mobile applies a child pornography filter provided by the Norwegian National Criminal Investigation Service.

In Germany the Commission for the protection of minors in the media (Kommission fur Jugendmedienschutz – KJM) was established in terms of legislation, the Jugendmedienschutz Statsvertrag. The KJM is obliged to oversee technical preventative measures, license self-regulatory bodies and approve technical measures such as content filtering and rating systems. This is a model of regulated self-regulation and contributes to the establishment of equal protection standards.

South Africa is currently in a position where there are various pieces of legislation applicable to the mobile communications industry, some relating to content, others to licensing and equipment and others to the operation of the business. Statutory bodies have been established in terms of the legislation which government could retain some jurisdiction over the industry. One instance where this measure can be employed is for the Minister to set appropriate standards for an IRB to comply with in terms of section 71 of the ECT Act. The Minister has to recognise an IRB before membership to the IRB will limit the liability of a service provider. The Minister can use this power to force necessary changes with respect to the procedures and standards of the IRB. This legislative tool can be used very effectively to force IRBs to engage with stakeholders outside of the industry.

Furthermore, the argument for a co-regulatory model in South Africa is strengthened by the fact that peer-to-peer communication is a major source of concern with respect to the use of mobile phones. The effective regulation of this type of communication requires some intervention from government, because there is a general prohibition on the interception and monitoring of the communications of individuals. The Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Interception Act) provides for exceptions to the general prohibition on interception and monitoring of communications. The exceptions relate to, amongst others, when interception –

- is authorised by a party of the communication
- takes place with the consent of a party to the communication
- is connection with carrying on of a business
- takes place to prevent serious bodily harm
- is undertaken for the purposes of determining location in case of emergency

These exceptions do not appear to be able to be employed in addressing bullying and grooming as harmful peer-to-peer communications. The Interception Act may need to be amended to broaden the application, to make it useful for combating this very personal form of communication. There is, however, a fine line between violating a person's right to privacy of communications and protecting them from potentially harmful communications. Therefore, the most workable solution with respect to this type of communication may not be legislation, but self-regulatory tools such as blocking mechanisms.

The Act also contains onerous provisions with respect to information that must be recorded and stored by the telecommunications service provider before a consumer may use a mobile telephone or before a SIM card is activated. The legislative measures could be employed in regulating the industry and protecting consumers. Industry has vehemently opposed these provisions because it will be a costly exercise. However, government has re-affirmed the provisions by proposing hefty penalties in the Interception Amendment Bill for anyone found not in compliance with provisions requiring the retention of consumer information.

Any regulatory model also requires an independent body to deal with complaints. Ideally, the body dealing with appeals and complaints should function as a quasi-judicial body, independent and seen to be independent from the industry and government. Its decisions should be open to be taken on review to the Supreme Court of Appeal.

A combination of statutory and self-regulatory measures may be the best way of ensuring an appropriate level of recognition, thus support, from government and buy-in by consumers.

3.3 Awareness and Education

Being informed of the possible problems that can arise when a child uses a mobile phone is a very important element of addressing the concerns. The importance of raising awareness and educating consumers cannot be overstated. Particularly with respect to since user-generated content which cannot and should not, ideally, be regulated by government. Consumer education needs to be implemented at every level:

- Industry; through booklets, advertisements, at points of sale

- Education authorities; institutionalized education, responsive curricula
- Civil society and consumer lobby groups
- Media; informative, factual and unbiased reporting

The education of mobile phone users could start at the point where a mobile telephone is purchased. Vodacom has published a parents' guide to cell phones. The guide deals with ways to pay, the emerging technologies, services provided via cell phones, malicious communications, content control and advice on location-based services, amongst others. An information booklet such as this one is an important step in raising awareness about the potential dangers which accompany mobile phone usage.

Netucation has published a Parents' Guide to Mxit. The guide has been in circulation since November 2006. The guide contains important and relevant information on what the technology entails, how to use it safely and how its use can impact on relationships. By giving talks at schools to parents and teachers, it has been found that by empowering adults with the knowledge they feel more at ease in addressing and interacting with children and adolescents on the safe use of the technology.

Government also has a role to play in this regard. The curriculum for Life Orientation, a subject taught from Grade 1 to 12, should include matters relating to the safe use of technology. Suggestions also included a type of standardized computer education for all school-going children. In the United States certain state laws require schools to have curricula on Internet safety as part of their Internet authorized use policies. Two of the leading curriculums used by schools are the I-safe programme and the Netsmartz curriculum.

Education campaigns targeted at teens are most effective when they are multi-faceted. An education campaign in schools should be accompanied by multi-media campaign encompassing print, radio and television components. One such campaign was launched in the United States in 2004. It started off by educating parents about on-line dangers and encouraging greater supervision of children's Internet usage. The following year advertisements warned teens about the dangers of establishing blind relationships. And the final round of advertisements to be launched in 2007 targets teenage girls advising them of the dangers of posting personal information online.

The question remains, however, how to reach adults who are not reached though institutionalized education programmes. Netucation and Vodacom's parents' guides are steps in the right direction; however, all mobile operators should be required to provide more information to users at the point of sale and at any other point of contact. Information relating to the codes of conduct that are in place, consumers' rights to complain and receive redress and how to go about complaining can be provided in advertisements of both Wireless Application Service Providers (Wasps) and mobile operators, on phone bills and pre-paid vouchers.

Handset manufacturers can also employ the benefits of having a captive audience and raise awareness by including a compulsory tutorial on the safe use of mobile technology before a telephone is activated.

Information about legislative and other measures that are in place should be publicised. A possibility in this regard is a booklet commissioned by the Department of Communications, setting out all legislation affecting this matter, combined with government and regulatory efforts in place and underway. This booklet must include details about the child pornography hotline, operated by the FPB, the office of the interception centres, cyber inspectors and the notification and take down procedures, amongst others.

4 Possible Responses for South Africa - Co-regulation

It appeared from the focus group and our research that a co-regulatory regime is preferable in South Africa; a regime that allows for participation by government and civil society, employs the regulatory mechanisms currently provided for in the legislation, but leaves the day-to-day regulation to suitably qualified industry representative bodies. Co-regulation is also the most suitable response in an industry with rapidly changing technology, because, on the one hand, one requires the skills and expertise of the industry to inform and standardise government policies and, on the other hand, government is needed to temper the exigencies of the market.

The measures provided for by legislation include:

- Recognition of IRBs by the Minister (ECT Act)

- Exceptions to interception and monitoring provided for in the Interception legislation (Interception Act)
- Classification of content by the FPB (FP Act)
- Notice and take-down procedures (ECT Act)

The appointment of an independent classification body appears to be central to the establishment of an effective co-regulatory regime. Classification requires an entity to be designated to define age categories and rating criteria, one to rate content and one to deal with disputes and complaints. The independence of a classification body is important. It has also been shown that consumers want access to lists of banned content. These factors need to be taken into account when the industry in consultation with government and civil society decides on the constitution of a classification body.

Classification also requires a different entity to define age categories and rating criteria. The FPB, informed by wide public consultation, can play a role in this regard. An amendment to the Films and Publications Act currently before Parliament aims to bring content on mobile phones and interactive games under the purview of the Act.

Once age categories are adopted and classification is complete, it is important also to specify the rating criteria and ensure that the criteria are applied consistently and fairly. It is also important to ensure that the rating is done by appropriately qualified persons.

Once rating is achieved, measures need to be adopted to filter and block harmful and illegal content. Various technical and regulatory measures can be employed in this regard, including filtering and blocking mechanisms and notification and take-down procedures.

Filtering and blocking is achieved by various technical means, some deployed at the network level and some within mobile communications devices. If technology is deployed at the network level, it will be necessary to determine whether consumers will be required to opt-out or opt-in of blocking devices being applied to their mobile phones. Opt-out is more burdensome for the consumer, requiring users to request that access to particular content not be allowed. Opt-in is where the user has to specifically request access to certain blocked content.

With both methods, there is a need for effective age verification systems. With the current and proposed amended provisions to the Interception Act requiring detailed information to be kept in respect of anyone purchasing a mobile phone or a SIM card, telecommunications service providers will have enough information to accurately verify the age of the buyer. The information will not, however, confirm the age of the user.

Notice and take-down procedures can be employed after rating has taken place, in conjunction with filtering and blocking. Notice and take-down removes the offending content from the relevant server or servers. Parties that host content agree to or are required to remove it after a legitimate take-down notice has been received. Disagreements are dealt with after the take-down has occurred, avoiding costly litigation at the expense of the consumer. This method is provided for in section 77 of the ECT Act.

This potential solution provides a great deal of control in the hands of the consumer (assuming the content host cooperates). As with the actual implementation of blocking technology, a great deal of consumer awareness will be necessary in order for the strategy to work effectively.

5 Conclusion

What has emerged clearly from this process is that it is still early days with respect to the effective co-regulation of the industry, specifically regarding accessing harmful content and injurious behaviour, such as bullying and grooming. Effective measures to protect children from accessing harmful content or behaviour via mobile communications devices will have to be a multi-pronged approach. All interested parties must play their part - children, parents and those tasked with empowering and protecting children such as schools and children's non-governmental organisations (NGOs), players in the market place, including mobile operators, service providers, WASPs and handset manufacturers, as well as public authorities.

Although few NGOs have information communication technology (ICT) capacity and infrastructure, NGOs have traditionally been catalysts for change and this should be no different in the ICT industry. Informing NGOs and wider civil society on these issues, creating awareness and ensuring their active and continuous interest and involvement require sustained attention and effort. For this reason it is important that existing

initiatives are supported and resources are shared in order for the impact to be maximized.

South African NGOs that are active in the ICT policy and application sphere are the South African NGO Network (SANGONeT), the Community Education Computer Society (CECS), the Freedom of Expression Institute (FXI), the National Community Radio Forum (NCRF), SchoolNet South Africa, NetDay, Ungana-Afrika and Women'sNet. These NGOs address issues of access to technology, gender and ICTs, constitutional issues and technical maintenance.

Regional and international NGOs such as Amarc Africa, Association for Progressive Communications (APC), bridges.org, the Media Institute for Southern Africa (MISA), SchoolNet Africa and Southern Africa Communications for Development (SACOD) also have a presence in South Africa.

Other initiatives aimed at the raising awareness about ICT issues in the NGO sector include SANGONeT's Thetha ICT Discussion Forums and the annual SANGONeT ICTs for Civil Society Conference and Exhibition.

The issues raised in the focus group tended to focus around two major areas where civil society can get involved

1) Education and awareness
2) Effective implementation of existing regulatory provisions.

Interventions by LHR and stakeholders can take place at various levels. We suggest that LHR takes a step back and take the issue back to its core constituency, the public. Once the public's input has been canvassed, it will inform the direction which the process needs to take. During wider consultation, it will become clearer whether LHR should focus their energies on education and awareness or on lobbying government and industry. Although these courses of action are not mutually exclusive, it is important to focus limited resources on specific outcomes in order to yield the best result.

Below we outline various actions which LHR can take, but stress the importance of wider consultation and research to properly guide the process going forward.

Get involved

Civil society organisations are often caught off guard because they wait for issues to be brought to them, either by government or the industry. In this fast moving industry, that scenario is unlikely. LHR and other civil society stakeholders need to be informed about legislative processes involving the industry, where and when they can make representations, thus raising their concerns and informing the debate. Attend public consultations and make well-researched and informed input.

At the moment two pieces of proposed amendments to legislation central to this issue are being considered. We have discussed both the Films and Publications Act Amendment Bill and the Interception ACT Amendment Bill. LHR must make recommendations as to the suitability of the proposed legislation to address the issue of children accessing harmful content on mobile phones.

A third piece of legislation which is at the final drafting stages is the Privacy and Data Protection Bill. This Bill seeks to protect the abuse of personal information, however as it was children's personal information are treated the same as that of adults. LHR should make representations to the effect that the abuse of children's personal information should be subject to heavier penalties.

It was made abundantly clear that Waspa's processes are only open to its members. In this regard, it is important that LHR acquires membership of the organisation in order influence the processes. A specific area where the voice of civil society is sorely lacking is with the adjudication panels. LHR should not only situate themselves in order to comment on Waspa's proceedings, but also provide them with a list of experts in the required fields who can be used as adjudicators.

Gaining membership to WASPA and other self-regulatory bodies will also be useful because the industry does not generally engage directly with civil society. In order to put civil society interests on the agenda, civil society must employ in the appropriate forums.

It is also important to remember that it is not necessary for LHR to reinvent the wheel; Netucation has published and is using a Parent's Guide to Mxit. They need to be supported to reach more schools and making the guide universally available.

Lobby government

A representative from the Department of Communications said during the focus group that less urgent matters are sometimes forgotten and intervention is required to put these back on the agenda. LHR and their partners can get involved in identifying legislative measures that have not been implemented or are not being effectively implemented and engage with the relevant government departments.

We have identified two specific issues which may require lobbying specific government departments, specifically the Department of Communications –

- Appointment of cyber inspectors
- Establishing regional interception offices.

Both these measures are provided for in the ECT Act, however since its inception only the Office for Interception Centres has been opened. These provisions were envisaged to provide law enforcement agencies with tools to combat crimes involving electronic communication technologies; however they need to be implemented first.

As our legislative process is a lengthy, complicated and political one, LHR and their partners will be well-advised not to lobby for specific pieces of legislation, but rather to endeavour for the implementation of what is already law.

Section 71 of the ECT Act requires that the Minister of Communications recognise an IRB before its members' liability can be limited in terms of section 72. In this respect, LHR can lobby the Minister to make mandatory specific issues that an IRB must comply with before it can be recognised. These include an effective age verification system which must be used by all its members. Another important aspect which can also be enforced by the Minister is that IRBs have transparent and participatory processes.

As regards education, LHR may want to lobby the education agencies to devise a curriculum for safe ICT use in schools. As this is still a relatively new field, the availability of teachers may be the first hurdle. However, this can be overcome by the implementation of self-teach curricula. These curricula embrace the natural curiosity and aptitude of children by encouraging them to teach themselves about the safe use of the technology. Netucation needs to be empowered in this regard.

The FPB can be more proactive in combating child pornography, which is only part of the problem. LHR can lobby for the creating on an online reporting mechanism. The

benefits of this type of reporting, it is anonymous, which most people prefer and it is more immediate than picking up a telephone.

Raise awareness

Raising awareness with the public requires input in a variety of ways – for example;

- Writing a well-researched opinion piece to stimulate public debate.

It is important to make use of any opportunity to raise the profile of the issue. Therefore, when a politician talks about regulation of social networking sites, it is vital to get a different opinion into the public domain as soon as possible.

- Using established email lists to keep people abreast of developments in the sector, and ask for their input.

Engage with stakeholders such as SANGONet to distribute a newsletter advising schools, parents and other stakeholders of the progress made with this issue, informing them of opportunities to have their own voices heard.

- Use the appropriate media.

Put up a blogspot where parents, caregivers, teachers, children and others can access professional advice on the issue.

Commission research

We have raised the lack of research as an obstacle to effective regulation. This needs to be addressed as a matter of urgency as any measures that are implemented will not have the benefit of a complete picture. Research must focus on not only the extent of the problem, but the emotional and psychological impact of addiction to social networking services, the effects of sexual solicitation and exploitation and cyber-bullying and cyber-threats.

This research will not only strengthen the response by LHR, it will also support the responsiveness of child protection and welfare agencies, such as Childline.

Wider public consultation

In conjunction with research, public opinion was canvassed during the European Commission's consultation process, by sending out questionnaires. Before LHR embarks on a campaign, it will be useful for their own purposes, to properly situate the concerns in a country where most human rights issues are still of the bread and butter variety. Canvassing the input of the wider community will serve LHR well when lobbying any public authority.

ANNEXURE B – Legal and Regulatory Framework

1 Current Legislative and Regulatory Framework

We now focus our attention on the current legislative and regulatory framework to see whether it is possible to address the concerns within the existing framework.

1.1 Constitution, 1996

The Constitution is the supreme law of South Africa. Law or conduct inconsistent with it is invalid. The obligations imposed by it must be fulfilled.

Chapter 2 of the Constitution, the Bill of Rights, is the one of the cornerstones of South Africa's democracy. Rights apply to all law and bind natural and juristic persons, the legislature, the judiciary, the executive and all organs of state. Section 28 provides that all the rights in the Bill of Rights apply to children. One of the rights that are entrenched in the Bill of Rights is the right to privacy. The right to privacy is an important human right, recognised around the world. It is dealt with in various international instruments, such as the United Nations Convention on the Rights of the Child and the International Covenant on Civil and Political Rights. Section 14 of the Constitution provides that:

> Everyone has the right to privacy, which includes the right not to have –
> (a) their person or home searched;
> (b) their property searched;
> (c) their possessions seized; or
> (d) the privacy of their communications infringed.

The right to privacy includes the right to privacy of communications. Therefore, any regulatory response which will seek to limit this right will have to consider the Bill of Rights.

Section 16(1) of the Constitution provides for the protection of free expression generally, and also specifically provides for freedom of the press and media, freedom to receive or impart information and ideas, artistic creativity, academic freedom and scientific research. Section 16(2) specifically excludes the rights extended in section 16(1) from

applying to propaganda for war, incitement of imminent violence or advocacy of hatred that is based on race, ethnicity, gender or religion, generally referred to as hate speech.

Any legislation or regulatory action which attempts to curtail rights will have to conform to the provisions of section 36 of the Constitution, the limitations clause. Section 36 provides that rights may be limited by a law of general application and then only to the extent that the limitation is reasonable and justifiable in an open and democratic society, based on human dignity, equality and freedom, taking into account all relevant factors. The factors are, amongst others -

- the nature of the right
- the importance of the purpose of the limitation
- the nature and extent of the limitation
- the relation between the limitation and its purpose
- less restrictive means to achieve the purpose

Reasonableness is an important consideration when applying the limitations clause. The Constitutional Court has held that there is no absolute standard for reasonableness, it has to be determined by balancing different interests. Thus the limitations clause analysis involves the weighing up of competing values and ultimately an assessment based on proportionality.

1.2 The Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002

The Regulation of Interception of Communications and Provision of Communication-related Information Act (Interception Act) was enacted to provide law enforcement agencies with the tools to combat crimes which involve the use of sophisticated communications technology. It regulates the interception and monitoring of communications in the public and private sphere. It repealed the Interception and Monitoring Prohibition Act, 1992.

In terms of the Interception Act, no person may intercept, or attempt to intercept or authorise another person to intercept, any communication, unless such actions falls within an exception provided for. Hereunder we focus on the exceptions that might be relied on for the lawful monitoring and interception of mobile communications.

The definitions set out in the Interception Act illustrate how wide the ambit of the Act is. Communications include direct (oral) and indirect (electronic) communications. Indirect communications includes downloading content from the Internet, SMS and e-mail, amongst others. Indirect communication is defined as –

> the transfer of information, including a message or any part of a message, whether –
> (a) in the form of –
> (i) speech, music or other sounds;
> (ii) data
> (iii) text
> (iv) visual images, whether animated or not;
> (v) signals; or
> (vi) radio frequency spectrum; or
> (b) in any other form or in any combination of forms,
> that is transmitted in whole or in part by means of a postal service or a telecommunications system.

Chapter 2 of the Interception Act provides for circumstances when the interception of communication can take place lawfully, when it -

1) takes place under an interception direction
2) is authorised by a party of the communication
3) takes place with the consent of a party to the communication
4) is connection with carrying on of a business
5) takes place to prevent serious bodily harm
6) is undertaken for the purposes of determining location in case of emergency
7) is authorised by certain other Acts; or
8) the monitoring of signal is for the purposes of installation or maintenance of equipment, facilities or devices; or
9) monitoring of signal and radio frequency spectrum, for purposes of managing radio frequency spectrum.

The fourth exception, is the business purpose exception. This exception authorises any person, in the course of carrying on a business, to intercept indirect communications –

- by means of which a transaction is entered into, or
- which otherwise relates to that business, or
- which otherwise takes place in the course of carrying on that business.

If an indirect communication relates to the business as set out above, it may be intercepted only with the consent of the system controller and for the purposes of monitoring or keeping a record of indirect communications:

- in order to establish the existence of facts,
- for purposes of investigating or detecting the unauthorised use of the telecommunications system, or
- where interception and monitoring is undertaken to secure, or as an inherent part of, the effective operation of the system.

The communications system concerned must be used, wholly or in part, in connection with that business, and lastly the system controller must have made all reasonable efforts to inform a person who intends to use the communications system concerned, that communications may be intercepted.

The fifth exception provides that any law enforcement officer may, if a party to the communications caused, or may cause, or threatened to cause bodily harm to another person, intercept communications or orally request a telecommunications service provider to route duplicate signals of the communications as specified in the request. The threat of injury needs to be immediate.

The sixth exception similarly provides for law enforcement officers to orally request interception and routing of communication for the purpose of determining a location in the case of an emergency. The person who the emergency relates to does not need to be a party to the communication.

These sections may be useful when law enforcement agencies are required to deal with persons who engage in acts that prepare a child for illegal, often sexual, activities. These activities can take place over mobile phones and include legal and illegal activities such as showing children pornography or persuading them to reveal personal information. Information is then used to abduct children or otherwise cause them harm.

The Interception Act also places obligations on service providers to obtain and retain detailed information with respect to any person who enters into a contract with a mobile cellular telecommunications service provider, as well as a consumer who only buys a cellular telephone or a SIM-card. In terms of section 39, a mobile operator must obtain the following information from any natural person with whom they wish to enter into a contract –

- full names, identity number, residential and business or postal address and
- a certified copy of his or her identification document.

The mobile operator must retain all this information, including the telephone number allocated to the person concerned and any other information which may be required to identify such person.

In terms of Chapter 6 of the Interception Act, the Minister of Justice in consultation with the Ministers of Communications, Safety and Security, Defence, Intelligence, Policing and national financial matters, must, at State expense –

(a) establish one or more centres, to be known as interception centres, for the interception of communications in terms of this Act;
(b) equip, operate and maintain such interception centres;
(c) acquire, install and maintain connections between telecommunication systems and interception centres; and
(d) administer the interception centres.

The Office for Interception Centre (OIC) was established in June 2006. The office acts on interception and monitoring directives granted as court orders by the High Court of South Africa. No other interception centres have been established. The OIC works closely with all telecommunications service providers.

There is currently an amendment being proposed to the Interception Act. The amendment seeks to strengthen the provisions in the Act relating to the information that must be kept in respect of cellular phone and SIM-card users. The bill proposes fines of up to R100 000 to be imposed on telecommunication service providers for every day that they fail to comply with the section relating to the information that must be kept. The current provisions as well as the amendments have raised objections from the industry as the industry is required to shoulder the financial burden.

1.3 The Films and Publications Act, 1996

The FP Act provides for the manner of distribution and exhibition of certain films and publications by classifying them. Despite the title of the Act, it is applicable to all electronic communication. Publication is defined as, inter alia –

…

any message or communication, including visual presentation, placed on any distributed network including, but not confined to the Internet

Data, including video, and voice conveyed via a mobile communications network is subject to the classification of the Film and Publication Board (FPB).

Classification of publications and films is only undertaken in response to a complaint or an application by a potential distributor. Thus a distributor applies for classification to the FPB, which determines the manner of a film or publication's distribution and exhibition. Classification can also be undertaken in response to a complaint. Therefore anyone may cause pornographic or violent material, for example, to be rated by bringing a complaint.

An Internet service provider is defined in the FP Act as 'any person who carries on the business of providing access to the Internet by any means'. Mobile operators may very well fall within this definition. Therefore we consider the obligations that the FP Act imposes on ISPs. Section 27A requires that every ISP register with the FPB and take all reasonable steps to prevent the use of their services for the hosting or distribution of child pornography. If an ISP has knowledge of illegal activities, it is obliged to disable access to the infringing material, report the presence thereof and preserve evidence for the purposes of investigation and prosecution by the relevant authorities. ISPs are also obliged to provide the South African Police Service with the particulars of users who gained, or attempted to gain access to, an Internet address that contains child pornography.

The FPB was established as a classification body, under the 1996 Act. Its stated purpose was to regulate the distribution of certain materials by means of classification. The 1999 Amendment broadened the ambit of the Act, and brought the creation, production, possession and distribution of certain publications and certain films into the ambit of the Act. The classification function of the FPB serves a useful purpose, as most regulatory models depend on an independent classification body.

The 2006 Amendment Bill is attempting to broaden the application of the FP Act further, by including the content regulation of broadcasting. The regulation of broadcasting is the responsibility of the Independent Communications Authority of South Africa (Icasa). The Broadcasting Complaints Commission of South Africa (BCCSA) deals with complaints with respect to broadcasting. The amendment has come under fire from media houses and freedom of expression advocates on the following grounds, amongst others.

- It subjects broadcasters to the control of the FPB, which does not meet the constitutional standard for independence as its members are appointed and paid by the Home Affairs minister.

- It treats “any sequence of visual images” as a “film”. The implication is that everything aired on television, from documentaries to news bulletins and sportscasts would have to undergo prior rating by the FPB, and a vast range of material would potentially be banned due to vague wording.
- Criminal offences detailed in the Bill violate freedom of expression and go too far in prohibiting legitimate expression.

The amendment also seeks to bring mobile phone content and interactive computer games into the purview of the Act. The Bill has been subject to public input at hearings on 3 and 4 May 2007 at Parliament in Cape Town. We have been told that the Home Affairs Parliamentary Committee has invited further representations on 17 and 18 May 2007.

The FPB currently operates a hotline to report any pornographic material involving children. The hotline is operational during office hours only with one person manning the phones and another one doing content analysis. There are plans underway to extend the hours of operation. The FBP works closely with Childline, STOP as well as the sexual family offences unit in the South African Police Service. The FPB Hotline receives referrals from these organisations, as well as makes referrals to them. The hotline does follow-ups with referral organisations.

1.4 The Electronic Communications and Transactions Act, 2002

The Electronic Communications and Transactions Act (ECT Act) was enacted to provide legal certainty with respect to electronic communications and transactions. In this section we examine the provisions dealing with unsolicited commercial communication or spam, the limitation of liability of service providers and data protection measures.

The ECT Act deals with spam in section 45. The problems associated with spam include objectionable content, misuse of recipient resources and a threat to email and Internet security. One aspect of the definition of spam is that the communication must be unsolicited, meaning no prior relationship existed between the recipient and the sender. The ECT Act also includes commerciality as a requirement of spam. This means that newsletters, religious messages, urban legends and the like, do not qualify as spam.

The ECT Act does not include 'bulk' in its definition, implying that a single unsolicited commercial electronic communication qualifies as spam.

The ECT Act provides that a sender of spam must provide the recipient with an option to cancel his or her subscription. The sender must also provide the recipient with identifying particulars of the source who provided the sender with the personal information of the recipient. Any person who contravenes this section is guilty of an offence and liable to penalties prescribed by the Act.

Chapter XI of the ECT Act provides for the limitation of liability of service providers. The term service providers mean 'any person providing an information system services'. The term 'information system' means a 'system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet'. The term 'information system services' is defined as including:

> the provision of connections, the operation of facilities for information systems, the provision of access to information systems, the transmission or routing of data messages between or among points specified by a user and the processing and storage of data, and the individual request of the recipient of the service

Sections 73-76 limit service providers' liability for acting as mere conduits, caching, hosting and providing information location tools, respectively. A service provider's liability is, however, only limited if that service provider belongs to an industry representative body recognised by the Minister of Communications and adheres to that body's code of conduct. Mobile operators, ISPs and WASPs qualify as service providers, therefore the provisions of Chapter XI which provides for the limitation of liability would apply to them.

Service providers are required to comply with notification and take-down procedures as provided for in section 77 of the ECT Act in order for their liability to be limited. The requirements for notification and take-down are in the SA Cellular Code of Good Practice, the ISPA and WASPA codes of conduct.

The ECT Act provides limited protection relating to personal information collected by electronic means. Section 51 of the Act provides that a person, who collects information by electronic means, may voluntarily subscribe to principles in the Act intended to protect a person's privacy. The principles are that a person must:

- obtain the written consent of a data subject for the collection and processing of personal information;

- disclose in writing, the purpose for which the information is being sought;
- not use the personal information obtained for any purpose other than the disclosed purpose;
- destroy any information which becomes obsolete; and
- not disclose to any third party any personal information held by it unless required by law or so authorised by the data subject.

Information collected by mobile operators may not be used for purposes other than the stated purpose for which it was collected. Therefore, subscribers to mobile services should not as a result of such subscription be inundated with unsolicited, commercial communications. A variety of measures had to be employed to deal with the spam in context of email, such as filters and blocking mechanisms. The protection of personal information is a good start, but it will probably not be sufficient to deal with the problem of spam in the context of mobile communications.

Section 80 of the Electronic Communications and Transactions Act (ECT Act) provides for the appointment of cyber inspectors. They may, in terms of the Act,

> monitor and inspect any website or activity on an information system in the public domain and report any unlawful activity to the appropriate authority

The cyber inspectors may assist any statutory body, such as the South African Police Service with any investigation. A court may issue a cyber inspector with a warrant authorising, without prior notice, the inspection, search or seizure of an information system that has a bearing on an investigation.

No cyber inspectors have been appointed to date.

1.5 Electronic Communications Act, 2005

The Electronic Communications Act (EC Act) came into force on 19 July 2006, repealing the Telecommunications Act, the Independent Broadcasting Authority Act and most of the Broadcasting Act. The primary object of the EC Act is to regulate electronic communications in the public interest and for that purpose to, amongst others, promote and facilitate convergence of telecommunications, broadcasting and information technologies.

The Act provides for three types of services:

- Electronic communications network services (ECNS);
- Electronic communications services (ECS); and
- Broadcasting services, and
- Services exempted from licensing.

In addition to the service licenses, licensees will require a radio frequency spectrum licence. The service licenses can fall into two categories: class or individual. The Independent Communications Authority of South Africa (Icasa) may prescribe further subcategories of services.

The EC Act provides for the conversion of all licences issued under the previous licensing regimes. The licences which will be converted include, amongst others, the MCTS, the public switched telecommunications service provider (PSTS), Telkom and Neotel, and the value-added network service providers (Vans). Under their current licences these three categories of licensees all have a right to provide services and a right to operate networks or facilities. These rights will be converted into ECNS and ECS licenses. As a result of the platform- and technology-neutral licensing regime provided for in the EC Act, it is possible that service providers may offer different services than the ones initially contemplated.

In terms of section 92(2) or 92(5) of the EC Act, Icasa deems service providers, such as resellers or WASPs, to have licence exemptions therefore they may continue to provide the services that they provide. Even though it is likely that resellers and WASPs will fall outside the licensing regime prescribed by the legislation, Icasa may prescribe terms and conditions that will apply to them.

Section 54 provides that the Authority (Icasa) must prescribe regulations setting out codes of conduct for licensees. Licensees under the EC Act will include anyone who provides an electronic communications network service (ECNS), an electronic communications service (ECS) or a broadcasting service. The codes may address any matter which is of concern to end-users and subscribers.

No codes have been prescribed in terms of section 54 of the EC Act.

1.6 Consumer Protection Bill

The Consumer Protection Bill is expected to be tabled in Parliament in 2007. The bill is a voluminous document of almost 200 pages and one of its earliest criticisms has been that it if a consumer has read it, they probably don't need it.

This section will focus on the objects of the bill and fundamental consumer rights set out in Chapter II of the bill

The objects of the bill is to promote and advance the social and economic welfare of consumers in South Africa by, amongst others –

- establishing a legal framework for the achievement and maintenance of a consumer market that is fair, accessible, efficient, sustainable and responsible
- protecting consumers from unfair and unreasonable trade practices and deceptive conduct
- improving consumer awareness and encouraging informed consumer choice and behaviour

The Bill sets out fundamental consumer rights in Chapter 2.

First, the right to equal access to the consumer market is provided for. This right includes protection against any discriminatory practices. In section 9, however, reasonable grounds for the differential treatment of consumers are set out. This section provides that it is not unfair discrimination on the basis of age to refuse to supply access to any goods or service to a minor or to require the consent of a parent or guardian. For example, if a regulatory response requires filtering and other mechanisms to be applied to minors' mobile phones to prevent them from accessing adult content, it will not be regarded as a discriminatory practice.

Part B of Chapter 2 entrenches the right to confidentiality and privacy. This right entitles a consumer to confidential treatment and prohibits a supplier from using confidential information supplied by the consumer in any manner which the consumer has not consented to. The consumer also has the right to restrict unwanted telecommunications access. This right is viewed as an extension of the consumer's right to privacy, therefore a consumer may refuse to accept or preemptively block any electronic communication which is mainly for the purposes for marketing or fundraising.

The Bill provides for the establishment of a register in which consumers can register a pre-emptive block, either generally or for specific purposes.

A consumer's right to choose is recognised in Part C. This right includes the right to select suppliers and products, the right to examine goods and to authorise services.

Other rights included in the Bill are the consumer's rights to:

- disclosure and information
- fair and responsible marketing and promotion
- honest dealing and fair agreements
- fair value, good quality and safety
- supplier's accountability
- to be heard and obtain redress

The Bill also provides for the protection and enforcement of consumer rights, the role of civil society, industry regulation and the establishment of National Consumer Protection Institutions.

1.7 Privacy and Data Protection Bill

The Privacy and Data Protection Bill is expected to be tabled in Parliament in 2007. In this section we will briefly look at the objects of the bill as well as the wide meaning given to ‘personal information’ and the eight principles which must inform the processing of personal information by public and private bodies.

The objects of this Bill are –

> to give effect to the constitutional right to privacy –
> (i) by safeguarding a person's personal information when processed by public and private bodies;
> (ii) in a manner which balances that right with any other rights, including the rights in the Bill of Rights in Chapter 2 of the Constitution, particularly the right to access to information;
> (iii) subject to justifiable limitations.

This Act, basically, provides for the limitations clause enquiry, in terms of section 36 of the Constitution. The limitation enquiry relates to the limitation of a fundamental right, such as privacy. The enquiry entails, when a fundamental right is limited, asking whether

the limitation is justifiable in democracy based on human dignity and equality, and secondly whether the same effect is possible by less restrictive means.

Personal information is a given a wide ambit, including any information relating to:

- race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- education or the medical, criminal or employment history of the person or information relating to financial transactions in which the person has been involved;
- any identifying number, symbol or other particular assigned to the person;
- the address, fingerprints or blood type of the person;
- the personal opinions, views or preferences of the person, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the person;
- the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the person, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and
- the name of the person where it appears with other personal information relating to the person or where the disclosure of the name itself would reveal information about the person,
- excludes information about a natural person who has been dead, or a juristic person that has ceased to exist, for more than 20 years.

This section widens the traditional arena in respect of which a person would have been entitled to expect protection.

Chapter 3 provides eight principles which must govern the processing of personal information.

- The first is the processing limitation which relates to the lawfulness of processing. This condition requires that processing must
    - take place in accordance with the law,

    - with the consent of the data subject and subject to certain other conditions as prescribed by the law.

  Processing is further limited by the principle which requires that any processing of personal information is not excessive.

- The second principle requires that collection and processing must be for a specific, explicitly defined and legitimate purpose and the data subject must be aware of the purpose of collection and the intended recipients.

- The third principle limits further processing in a way incompatible with the purpose for which it has been collected in terms of the afore-mentioned principle.

- The fourth principle relates to the quality of information; it entails ensuring that personal information is complete, not misleading, up-to-date and accurate.

- The fifth principle requires that personal information may only be collected by a responsible party that has notified the appropriate authorities and the data subject.

- The responsible party is also required to implement the necessary security measures to ensure the integrity of personal information.

- The seventh principle requires that the individual has access to any personal information as well as the right to the correction of information.

- The last principle requires the responsible party to ensure that the measures that give effect to the principles set out in this chapter of the Bill are complied with.

The Bill provides for exemptions on the prohibitions of the processing of various types of personal information, as well as exemptions from the principles. It provides for the establishment, staffing, powers and functions of the Information Protection Commission.

This Bill echoes the principles of data protection provided for in the ECT Act. The ones in the ECT Act are voluntary, whereas this bill provides for definite prohibitions on the processing of various types of personal information.

Children's personal information is not treated distinctly in the proposed legislation; however the data protection principles contained in the Bill are in line with international trends regarding data protection. In April 2007 the Department of Justice was receiving comments on the Bill. Mark Heyink of Information Governance, a participant at the focus group discussion, made representations to the effect that knowingly processing the personal information of data subjects under 18 years, without the consent of parents or legal guardians should be criminalized. Further, in the event of a data processor breaching the duties imposed in terms of the principles, provided for in the Bill, resulting in the compromise of the personal information of a minor data subject, the penalties imposed must be more severe.

ANNEXURE B – List of Focus Group Attendees

Name of organization	Persons attended	Email address
Lawyers for Human Rights	Nesira Singh	nesira@lhr.org.za
	Saskia Welschen	siwelschen@hotmail.com
Lisa Thornton Inc	Lisa Thornton	lat@thornton.co.za
	Carmen Cupido	cjc@thornton.co.za
Waspa	Leon Perlman	leon@waspa.org.za
Youth Dynamix	Andrea Kraushaar	Andrea.kraushaar@youthdynamix.co.za
Child Line Gauteng	Lynne Cawood	directorgauteng@childline.org.za
	Henry Muchauraya	infogauteng@childline.org.za
SA Human Rights Commission	Tom Manthata	smanjoo@sahrc.org.za
	Shameme Manjoo	
Barend Burgers Attorneys	Barend Burgers	barendb@bbatt.de
Information Governance Ltd	Mark Heyink	mark@heyink.co.za
Child Welfare SA	Beena Chiba	Gauteng1@childwelfaresa.org.za
	Bharti Patel	
Department of Justice	Delleen Clarke	dclarke@doj.gov.za
FXI	Simon Delaney	Simon.delaney@fxi.org.za
Dep. of Communications	Alf Wiltz	alf@doc.gov.za
Films & Publications Board	Antoinette Basson	antoinette@fpb.gov.za
Icasa	Councilor Zolisa Mazisa	zmazisa@icasa.org.za
MTN Group	Lovina Nunen	lovinan@mtn.co.za
Vodacom	Moshangane Manzini	manzinst@vodacom.co.za
Netucation/Mxit	Ramon Thomas	Ramon.thomas@netucation.com
Virgin Mobile	Janice Allem	Janice.allem@virginmobile.co.za
	Simone Kosmides	Simone.kosmides@virginmobile.co.za
Wireless Warriors	Richard Cimaidi	Richard@wirelesswarriors.co.za
Unisa	M Kabengele	lrsvanito@yahoo.fr

ANNEXURE C - Resources

Cyberlaw@SA (R Buys ed, 2nd ed Van Schaik Publishers 2004).

European Commission: Information Society and Media Directorate-General, Consultation Paper and Summary Results of Public Consultation: Child safety and mobile phone services (16 October 2006); available online at http://ec.europa.eu/information_society/activities/sip/docs/public_consultation/public_consultation_rsults_en.pdf.

Oxford Internet Institute-led Working Group on Mobile Phones and Child Protection of the European Internet Co-regulation Network (EICN) (Christian Ahlert, Marcus Alexander and Damian Tambini), Implications of Mobile Internet for the Protection of Minors (April 2005); available online at http://www.forumti.it/fti/downloads/Ahlert_Nash_Marsden.pdf.

Programme in Comparative Media Law and Policy, University of Oxford Christian Ahlert, Marcus Alexander and Damian Tambini, European 3G Mobile Industry Self-regulation: IAPCODE Background Paper World Telemedia Conference (3-5 November 2003); available online at http://www.selfregulation.info/iapcoda/031106-mobiles-revised-bckgrd.pdf.

Telecommunications Law in South Africa (L Thornton et al ed, STE Publishers 2006); available online at *www.idrc.org.sg/en/ev-104793-201-1-DO_TOPIC.html*.

United Kingdom Code of practice for the self-regulation of new forms of content on mobiles (19 January 2004).