ISPs IN THE MIDDLE

An investigation of the role of Internet Service Providers in the regulation of the Internet and the law of specific application to Internet Service Providers in South Africa

Submitted by: Dominic Cull (CLLDOM001)

Supervisor: Professor Julien Hofman

Research dissertation presented for the approval of Senate in fulfilment of part of the requirements for the LLM in approved courses and a minor dissertation. The other part of the requirement for this qualification was the completion of a programme of courses.

I hereby declare that I have read and understood the regulations governing the submission of LLM dissertations, including those relating to length and plagiarism, as contained in the rules of this University, and that this dissertation conforms to those regulations.

EXECUTIVE SUMMARY

One of the primary difficulties in undertaking an examination of the role and regulation of Internet service providers in South Africa is attempting to understand exactly what is meant by the terms "Internet service provider" or "service provider" when these are used in a regulatory context. The importance of this definition cannot be understated as it will determine the scope of application of regulatory measures – who will have to comply with legislated obligations or be able to take advantage of statutory exemptions, and how will this affect the effectiveness of measures undertaken?

It will be seen that the current definitions at play in South Africa are extremely ambiguous and support an interpretation which is sharply at odds with the common or traditional perceptions of what constitutes an ISP. One implication of this ambiguity at a fundamental level is that there are many entities which are currently unaware of their classification as ISPs for certain legal purposes and which have in no way participated in the process of drafting legislation, regulations and directives which will directly impact on their service provision and economic viability.

In examining current and anticipated regulation of ISPs it is instructive to divide such legislation up into that which governs the physical structure of the Internet and that which governs the content found on or communicated through the Internet.

While control of physical access to the Internet provided by ISPs is provided by the Telecommunications Act, it has no direct bearing on unlawful activities perpetrated by end-users through such access. This paper will consider regulation of content under three specifically-applicable pieces of legislation – the Electronic Communications and Transactions Act 25 of 2002, the Regulation and Interception of Communications and Provision of Communication-related Information Act 70 of 2002, and the Films and Publications Act 65 of 1996 as amended by the Film and Publications Amendment Act of 2004.

It is concluded that ISPs stand on the brink of a fundamental shift in their role in society and that they will in future be required, in many respects, to further the interests of the State, often to the detriment of their position as custodian of the personal information of their clients to which they are privy. ISPs at an individual and industry level are going to be hard-pressed to cope with the quantity and complexity of the legislation that will regulate the activities which they undertake and, in turn, define many of the ways in which their customers conduct themselves with regard to their use of electronic communications.

1. INTRODUCTION

It is the express purpose of this paper to examine the increasing identification of Internet service providers (ISPs) as a vital focal point in the regulation of the Internet and the implications which this has for persons carrying on the business of an ISP. While the law currently impacting on ISPs in South Africa remains underdeveloped, the last month alone has seen the release of a number of vitally important Acts, draft directives, notices and proposed regulations. Two years ago, it should be remembered, there was no specific law dealing with electronic communications at all.

It is submitted that there is now a strong case for identifying the law pertaining to Internet service providers and related entities as a distinct subset of the law governing electronic communications. Indeed it will be fascinating to observe the manner in which "ISP law" in South Africa continues to develop as the authorities grapple with the issues flowing from the unique nature of ISPs and the roles which they perform, both in the regulation of the Internet and society as a whole.

It must be emphasised that the author has not, in general, attempted to offer an opinion on the broad constitutional issues which legislation such as RICA will bring into focus, although this will be an important element of the future strategy of ISPs. There should be little doubt that RICA, as discussed below, is susceptible to a challenge that it unjustifiably limits the rights which South Africans enjoy to the privacy of their communications.

Rather the focus is on actual and concretely anticipated legislative measures to regulate ISPs – the following is rooted in the perspective of ISPs.

2. PERSPECTIVES ON THE ROLE OF INTERNET SERVICE PROVIDERS IN THE REGULATION OF THE INTERNET

ISPs are the crucial intermediaries in almost every aspect of communication through the Internet – they are the conduit through which online communications flow and as such are in a position of unparalleled power in terms of the private information which they hold. Advances in technology have facilitated access by ISPs to just about everything that their clients (and others) do when online.

As a result of this positioning and user dependence on their services, users are being forced to place ever greater reliance on ISPs to safeguard their communications and personal information from others, be they of a public or private nature. Users generally have no choice but to believe that ISPs will respect the privacy of their communications and information[1]. It is this trend which has led to the enactment of data protection legislation - such as the EU Data Protection Directive – that seeks to place obligations on ISPs and others to delete or anonymise customer information unless retention is required for lawful purposes.

This has occurred within the context of the Internet as a tool for facilitating freedom of expression, attributable in the most part to the convenience, immediacy, perceived security and anonymity with which online communications take place. As a result ISPs are the custodians of an accumulation of data which has inevitably come to the attention of a large number of governments.

[1] see Kerr, I & Gilbert D "The changing role of ISPs in the investigation of cybercrime" in Information Ethics in an Electronic Age: Current issues in Africa and the world, ed. Thomas Mendina & Johannes Britz (Jefferson, North Carolina: McFarland Press, 2004 (available from http://www.jisclegal.ac.uk/ispliability/ispliability.htm last visited 12 Sept 2004)

Massive data holdings are not, however, restricted to entities which we would generally regard as ISPs. The common understanding of the descriptive "Internet service provider" is typified in South Africa by entities such as MWeb or UUNet, an understanding which holds within the "ISP" industry itself as can be seen by the entities which have applied for membership of the Internet Service Providers Association (ISPA)[2].

But, as will be seen below, the definition of ISP for the purposes of the regulation of the Internet is generally cast much wider than this traditional perception. Financial, insurance, medical and educational institutions are also holders of vast quantities of personal information and most governments have sought to extend the application of laws regulating the Internet to cover these bodies as well.

The South African government is no exception. The Regulation of Interception of Communications and Provision of Communication-related Information Act[3] ("RICA") is positioned to be the central instrument in allowing law enforcement and government agencies access to the information held by ISPs for the expressed purpose of addressing security and crime, particularly post September 11 2001.

Kerr and Gilbert[4] succinctly identify the tension between the two distinct roles assumed by ISPs - ISPs have to intermediate between being the custodian of personal information and protector of privacy as against the potential value of such information for law enforcement.

The dominant thinking when considering the adaptation of laws of general application has been to position ISPs as "mere conduits", thereby equating them for legal purposed with traditional telecommunications service providers that passively allow transmission of communications data without creating or altering the data being carried.

The rationale behind this approach was that it would be impractical and create a disproportionate economic burden for ISPs to be expected to monitor the services which they provide in such a manner as prevent criminal or illegal use. When considering the example of large ISPs, such as Yahoo or MWeb, it is evident that actively "policing" all web pages and other services to which they offer access would be an immense burden.

Implicit in this argument is the proponent's identification of the fundamental role of ISPs as intermediaries which facilitate the free-flowing nature of the Internet – any legal obligation or potential liability imposed on ISPs may have the effect of retarding this free-flow.

The "mere conduit" approach appears, however, to be under threat from a number of directions. Hayes[5] identifies the four primary issues facing ISPs in this regard as being:

1. content liability such as defamation
2. intellectual property rights
3. crime detection and monitoring
4. Jurisdictional exposure.

ISPs are simply too important in the context of electronic communications and transactions to ignore. They constitute the gateway to the Internet and the services which it offers and therefore can be said to be best placed to physically enforce regulatory objectives. On a civil law level ISPs are attractive as Defendants due to the relative ease with which they can be located as opposed to users, and the greater likelihood of their having the resources to satisfy an adverse judgement.

---

[2] see www.ispa.org.za and www.ispmap.org.za
[3] Act 70 of 2002
[4] see fn2
[5] Hayes, Martin J LLM "Internet Service Provider Liability"

Advocates of the erosion of the “mere conduit” principle argue that the direct regulation of ISPs and the manner in which they respond to abuses perpetrated on the Internet, will benefit users of the Internet by effectively restricting criminal and illegal activities. In other words any retardation of the free-flowing nature of the Internet is justified by enhancements in the safety of its use and the quality of the services which it provides. A related benefit is an expected boom in electronic commerce following improvements in consumer and business perceptions of safety and security when transacting on the Internet.

Most legislation relevant to the burden to be placed on ISPs enacted in the last decade, including the Electronic Communications and Transactions Act[6], has adopted a compromise position whereby an ISP can avoid liability by adopting and consistently implementing a “Notice and Take Down” procedure. The principle is that ISPs will not be automatically liable for illegal or infringing content or services where they act expediently to remove such content or disable access to such service upon proper notification of its existence.

In the context of crime and security legislation, however, there is an argument that the direct impact of acts such as RICA is to change ISPs from mere conduits into actual reservoirs[7].

3. THE PROBLEM OF DEFINITION

The term Internet Service Provider is generally used to describe an entity which provides a variety of Internet-related activity. A typical ISP will offer access to the Internet, host web sites on behalf of its clients and provide a news service and search engine capability, thereby performing the roles of access provider, host, content and navigation provider. The term is accordingly inherently ambiguous as it refers to a number of differing bundles of services which may be offered by one party.

The role adopted or nature of the service provided by an ISP at any point in time dictates the manner in which regulatory measures will apply to that ISP.

We turn now to a consideration of the different legal definitions of ISP currently at play under South African law.

3.1. Definition of “service providers” under the ECT Act

The term “Internet service provider” is not directly used or defined in the Act, but the term “service provider” is defined with specific application to Chapter XI of the Act – Limitation of Liability of Service Providers.

“In this Chapter, "service provider" means any person providing information system services.”[8]

By including the defined terms “information system services” and “information systems” a comprehensive definition of “service provider” can be reached, *viz*.

> "service provider" means any person providing services including the provision of connections, the operation of facilities for and the provision of access to a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet, the transmission or routing of data messages between or among

[6] Act 25 of 2002
[7] see fn 1
[8] ECT Act s70

points specified by a user and the processing and storage of data, at the individual request of the recipient of the service[9].

While the ECT Act definition, unlike the definition of "Internet service providers" contained in RICA, does not make mention of any requirement that a service provider should be licensed under Chapter V of the Telecommunications it is submitted that there is nothing in the definition which would justify a narrow interpretation limiting the scope of application of Chapter XI to licensed service providers.

Rather, it is submitted, it is the activities listed in Chapter XI – access provision, hosting, temporary information storage and navigational services – which provide substance to the definition of "service provider". As the definition applies specifically to Chapter XI there seems little point in regarding an entity not providing at least one of the listed activities as a service provider for the purposes of Chapter XI.

Nevertheless the definition provided is broad enough to cover a number of entities which would be extremely surprised to find themselves regarded as ISPs[10]. A business, for example, which provides a service whereby its employees may upload content to its intranet, is providing access to a system for generating, sending, receiving, storing, displaying or otherwise processing data messages. By implication it should, therefore, theoretically be competent for an aggrieved party to serve a take-down notice on that business.

As a matter of terminological clarification it should be noted that VANS operators, as providers of services encapsulated in the definition of "information system services", can be regarded as "service providers" for the purposed of Chapter XI.

3.2. Definition of "Internet service providers" and "telecommunications service providers" under RICA

Given the centrality of telecommunications and Internet service providers to the efficient functioning of RICA, the definition of these entities is critical in determining the parties who will be required to undertake certain actions in order to cooperate with law enforcement agencies. From the point of view of entities or persons which may potentially be regarded as ISPs the need for a clear definition laying out who will and who will not be regarded as ISPs for the purposes of the Act is essential given the criminal sanctions for non-compliance as the cost and operational implications of developing an interception capacity.

Under RICA the "Internet" is defined as "the international computer network known by that name"[11], while "Internet service provider" means

> "any person who provides access to, or any other service related to, the Internet to another person, whether or not such access or service is provided under and in accordance with a telecommunication service licence issued to the first-mentioned person under Chapter V of the Telecommunications Act".[12]

---

[9] s1 Definitions "information system" means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet;
"information system services" includes 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, at the individual request of the recipient of the service;

[10] see the discussion with regard to the definition of ISP under RICA for more in this regard

[11] RICA s1(1) definitions

[12] RICA s1(1) definitions

ISPs are furthermore subsumed under the definition of “telecommunications service provider”:

> "**telecommunication service provider** means any—
> (*a*) person who provides a telecommunication service under and in accordance with a telecommunication service licence issued to such person under Chapter V of the Telecommunications Act, and includes any person who provides—
> (i) a local access telecommunication service, public pay-telephone service, value-added network service or private telecommunication network as defined in the Telecommunications Act; or
> (ii) any other telecommunication service licensed or deemed to be licensed or exempted from being licensed as such in terms of the Telecommunications Act; and
> (*b*) **Internet service provider**.”[13]
>
> *(writer’s emphasis)*

The first point to draw from the definition of ISPs under RICA is that it was the clear intention of the drafters to make the scope of application of the Act as broad as possible in respect of ISPs. The possession of a valid VANS or other licence is irrelevant in determining whether an entity providing Internet access and/or related services will be required to comply with the Act. It is clear from portfolio committee minutes and submissions made during the drafting process that the drafters contemplated limiting the definition of ISPs to entities providing Internet access under and in accordance with a telecommunications licence.

If this course had been adopted then the inclusion of a definition for ISPs, as also the explicit inclusion of ISPs under the definition of TSPs, would have been unnecessary. By rejecting this argument it appears unequivocal that the legislature intended RICA to apply to a group wider than those doing providing Internet services under a telecommunications licence.

This definition is extremely broad, primarily as a result of the inclusion of the phrase “any other service related to the Internet”. This could conceivably encompass just about anything to do with the Internet, including the provision of content. If this definition is taken to its interpretative extreme the implication is that the provisions of RICA could apply to web site providers, anti-virus vendors and banks providing online banking services.

Moreover the RICA definition refers to the provision of services to “any person”. This could be taken to refer to employers allowing staff and independent contractors access to the Internet in order to facilitate the meeting of business objectives. It would include non-ISP providers such as ABSA, FNB and even some gyms which provide access to the Internet, as also schools and tertiary educational institutions providing access to learners and students.

In the view of Privacy International, commenting on the definition adopted in the Regulation of Interception of Communications and Provision of Communication-related Information Act (“RICA”):

> “[RICA] imposes significant burdens on an extremely wide range of private persons, organizations and companies. There are few, if any, computer or communications systems that would not fall under this definition. Every new communications tool and system would be required to implement surveillance capabilities.”[14]

It is submitted, however, that the context provided by the specific obligations on ISPs contained in RICA do not support such a broad interpretation. It surely cannot have been the intention of the

---

[13] RICA s1(1) definitions
[14] Letter to the Committee on Justice & Constitutional Development from privacy International dated 13 August 2001; available at http://pi.gn.apc.org/countries/south_africa/pi-sa-intercept-letter.html (last visited 22 September 2004)

legislature that, for example, all businesses providing internet access for their staff should implement an interception and storage capacity and otherwise comply with the extremely onerous technical requirements of the Act and the subsequent Directive?

A broad interpretation would also have the effect of making the Act practically unenforceable.

Certainty in this regard is highly desirable. Until such time as clarity has been obtained it would be advisable for all entities potentially affected by RICA to consider making application for an exemption from the requirement that they acquire an interception and storage capability at their own cost[15].

3.3. Definition of ISPs under the FPAA

It is an explicit object of the Act "to address the problem of child pornography on the Internet by bringing Internet service providers within the jurisdiction of the principal Act"[16].

The Act defines an Internet service provider as:

> "any person who provides access to the Internet by any means"[17],

while an Internet address is defined as

> "a website, a bulletin board service, an Internet chat-room or newsgroup or any other Internet or shared network protocol address"[18].

Concerns over the definition of Internet Service Provider in preceding Bills were expressed by a variety of parties.

In its submission[19] to the portfolio committee the Internet Service Providers Association (ISPA) criticised the "expansiveness" of the definition of Internet service provider, pointing out that the standing definition could be construed to include, inter alia, parents who pay an Internet subscription to allow children home access, schools and even the government itself through its provision of public access terminals (PITs). ISPA drew the distinction that all of these so-called ISPs are largely unregulated – they are not licensed under the Telecommunications Act or bound by any industry code of conduct.

This criticism was also included in the submissions of MTN, Cell C and during discussion in the portfolio committee.

ISPA's submission suggests that the committee considering the FPAA adopt the following definition of an ISP:

> "An ISP is a duly licensed holder of a value added network (VANS) licensees, pursuant to section 40 of the Telecommunications Act, 1996, as amended. We suggest that an alternative definition is used to describe "anyone else who provides access to the Internet by any other means."

A further definition suggested by one of the legal advisors to the committee during deliberations around the FPAA was that an ISP should be seen as "any person carrying on the business of Internet provision"[20]. The thrust of this argument is that there should be a commercial aspect to

---

[15] see below
[16] from Memorandum on the objects of the Films and Publications Amendment Act 2004
[17] section 1(d)
[18] section 1(d)
[19] found at http://www.pmg.org.za/docs/2003/appendices/031118ispa.htm (last visited 6 Sept 04)
[20] submission of Advocate Kellner found at http://www.pmg.org.za/docs/2004/viewminute.php?id=3846

the definition, i.e. that the provision of access to the Internet and/or e-mail should be for commercial gain.

3.4. Conclusion

This problem of definition is not a uniquely South African one – the same difficulties have been experienced in a number of other jurisdictions.

In the United States, for example, a broad definition is accorded to ISPs under the Digital Millennium Copyright Act[21]. The courts, however, in ascertaining whether an entity falls under the definition of a service provider for the purposes of qualifying for the safe harbour offered by the DMCA, have applied a relatively restrictive interpretation[22].

In Australia similar criticisms as to the breadth of the definition of ISPs has been raised against the Broadcasting Services Amendment (Online Services) Act of 1999[23]. The definition used is broadly similar to that employed in South Africa other than that "internet content hosts" are separately defined as persons hosting or proposing to host Internet content in Australia and there is a qualifier on the definition of ISP to the effect that the Internet service must be provided to someone outside of the "immediate circle" of the supplier[24].

This latter distinction is useful in that it would perforce exclude the scenarios of a business providing access to its staff (who would be within the immediate circle of the business), a parent contracting to provide access for a child and an educational institution providing access to students. It would not, however, exclude the provision of access by a business to an independent contractor who could be regarded as outside of the immediate circle of a business or a visitor to an educational institution who uses its Internet facilities.

Whether by accident or design, more probably the latter, the definitions of ISP adopted to date under South African law give the relevant pieces of legislation a far broader scope of application than is suggested by the use of the term Internet service provider. While a certain definitional fuzziness may be acceptable where ISPs are regarded as passive adherents to a law, compliance with which is voluntary, it is, it is submitted, intolerable where ISPs are required to undertake, positive, continuing and costly obligations and where severe penalties may be imposed for non-compliance.

It is submitted that the legislature needs to investigate and clarify the scope of application of the Acts discussed above as a matter of priority. Consideration should also be given to adopting a uniform definition which would apply across the board, thereby creating greater legal certainty.

It is further submitted that courts considering the various definitions should adopt a restrictive interpretation based on the intention of the legislature in enacting the abovementioned legislation, particularly where the interpretation will have a bearing on the applicability of criminal offences to entities.

For the purposes of, and in order to greatly simplify, much of the discussion below, references to ISPs will generally be intended to refer to ISPs as they are traditionally perceived – entities which contract with their clients for the provision of Internet access and closely related services, usually in exchange for the payment of a set fee. These are the entities which have the technical

---

[21] section 512

[22] see Fressendon "Safe Harbour Qualifying Providers" in IDEA – The Journal of Law and Technology 42 IDEA 391 (2002) at 398; available from http://www.idea.piercelaw.edu.articles/42/42_3/3.Fressenden.pdf (last visited 2 September 2004)

[23] available from http://parlinfoweb.aph.gov.au/piweb/Repository/Legis/ems/Linked/24060416.pdf (last visited 8 Sept 2004)

[24] Chalet, A & Testro, L "Are you an ISP? - Ambiguity in the Internet Censorship Legislation" available at http://www.isoc-au.org.au/Regulation/PFoxBSA.html (last visited 3 September 2004)

expertise and physical control which would be required to perform the majority of the legal obligations currently proposed or in force.

3. THE TELECOMMUNICATIONS ACT 103 OF 1996

The Telecommunications Act, 103 of 1996 (the "Act") provides the core regulation for all providers of telecommunication services in South Africa[25]. It regulates the physical component of the Internet in South Africa[26].

The Act defines telecommunication as "the emission, transmission or reception of a signal from one point to another by means of electricity, magnetism, radio or other electromagnetic waves, or any agency of a like nature, whether with or without the aid of tangible conductors"[27].

Based on the Act's definition, communications taking place via e-mail or the Internet constitute telecommunications. This would hold true even where the communications are transmitted over a wireless network.

The Act further defines a "telecommunication service" as "any service provided by means of a telecommunication system" and "telecommunications system" is defined as "any system or series of telecommunication facilities or radio, optical or other electromagnetic apparatus or any similar technical system used for the purpose of telecommunication, whether or not such telecommunication is subject to rearrangement, composition or other processes by any means in the course of their transmission or emission or reception"[28].

It is clear that the provision of an Internet service, including wireless provision, is a telecommunication service as contemplated in the Act, as it provides customers with the service of (at minimum) Internet connectivity over a telecommunications system.

The Act sets out requirements in respect of licensing of telecommunication service providers (TSPs)[29], the licensing or approval of equipment[30] and the licensing of frequency use[31] (relevant to wireless ISPs or WISPs).

The Independent Communications Authority of South Africa (ICASA)[32] is a notionally independent body charged with regulating*, inter alia*, the South African telecommunications industry in accordance with the procedures specified in the Telecommunications Act. ICASA is almost certainly under-funded and understaffed and has struggled to impose order in the industry while many parties have noted that the body lacks the will to effectively challenge Telkom in the area of anti-competitive practices.

Nevertheless, and as will be seen below, ICASA has been important in clarifying certain areas relating to ISPs as VANS licence-holders. The future capability of ICASA is crucial to the telecommunications industry given the liberalisation initiatives recently announced by the Department of Communications (DoC) (discussed below).

---

[25] Alhadeff, A and Cohen, M "Functionality of value-added network service providers and their liability" in Cyberlaw II, ed Buys, Van Schaik Publishers 2004 p233
[26] Alberts in Buys (ed), Cyberlaw I, 2000 p393
[27] Telecommunications Act s1 definitions
[28] Telecommunications Act s1 definitions
[29] Chapter V
[30] Chapter VI
[31] Chapter IV
[32] constituted by the Independent Communications Authority of South Africa Act 13 of 2000

3.1. Licensing

Section 32 of the Act prohibits the provision of a telecommunication service without a licence and it thus seems clear that no ISP can provide Internet connectivity and/or services without a licence[33]. Section 32 likewise provides that the telecommunications services that may be provided by a licence holder must be under and in accordance with a telecommunication service licence issued to that person and a licence shall confer on the holder the privileges and subject him or her to the obligations provided in the Act or specified in the licence[34].

The appropriate licence for an ISP is a Value-Added Network Services (VANS) licence under section 40 of the Act. After repeated calls for clarity as to the nature of VANS, a definition was inserted into the Act in 2001, *viz*.

> **"value-added network service"** means a telecommunication service provided by a person over a telecommunication facility, which facility has been obtained by that person in accordance with the provisions of section 40(2) of the Act, to one or more customers of that person concurrently, during which value is added for the benefit of the customers, which may consist of—
>
> (a) any kind of technological intervention that would act on the content, format or protocol or similar aspects of the signals transmitted or received by the customer in order to provide those customers with additional, different or restructured information;
> (b) the provision of authorised access to, and interaction with, processes for storing and retrieval of text and data;
> (c) managed data network services;"[35]

From the above definition and certain of the provisions of section 40 of the Act the following conditions for the provision of VANS are applicable:

(a) VANS licences to provide, *inter alia*, electronic data interchange (EDI), e-mail and access to a managed data network service or database must be endorsed with a condition that "the service in question be provided by means of telecommunications facilities"[36] provided by the Public Switched Telecommunications Service (PSTS) provider, i.e. Telkom[37].
(b) The service offered must add value to the telecommunications services ordinarily available to end-users, i.e. the service cannot merely constitute the resale of services offered by the PSTS provider.
(c) The services that can be provided under the Act are those listed in the definition but this is not a closed list.

Further clarification of what exactly constitutes VANS as opposed to PSTS was set out by ICASA in an explanatory memorandum[38] and in its determination in the Section 100 enquiry between Telkom SA Ltd and Internet Solutions[39]. In this matter it was held that "..the moment TCP/IP protocol is utilised, any conveyance of data which may occur falls outside of the realms of Telkom's PSTS rights and falls within the rights of VANS providers to provide". The logic behind this statement is that, whereas the use of TCP/IP is integral to the provision of VANS, it is not integral to the offering of a PSTS service. The importance of the ruling is that it clarified that the provision of Internet services is a VANS and not a PSTS.

---

[33] Telecommunications Act s32(1)
[34] Telecommunications Act s32(2)
[35] inserted by section 1(p) of Act 64 of 2001, effective November 2001
[36] Telecommunications Act s40(2)
[37] and, potentially, the Second National Operator (SNO); see note on the latest liberalisation policy announcement (below)
[38] "VANS/PTN Regulatory Framework", 1 June 2001
[39] available at http://www.icasa.org.za/Repository/Resources/Whats%20New/final%20IS-Telkom%20ruling.pdf (last visited 15 Sept 2004)

A further guide to the kinds of services which a VANS licence holder can provide is found in Telkom's VANS licence, which include, without limitation:-

(a) electronic data interchange;
(b) electronic mail
(c) protocol conversion;
(d) access to a data base or a managed data network service;
(e) voice mail;
(f) store-and-forward fax;
(g) videoconferencing;
(h) telecommunication related publishing and advertising services;
(i) electronic information services, including Internet service provision;

and any other telecommunication service (excluding Mobile Telecommunication Service and Public Switched Telecommunication Service) and in respect of which conveyance of is no more than is incidental to, and necessary for, the provision of that service'.[40]

Otherwise stated and as their nomenclature suggests, VANS are telecommunication services which have the effect of adding value to the conveyance of communications for the benefit of customers.[41] Once an end-user has gained access to the VANS network then he or she will be able to gain access to the Internet. When connected, the end-user will also be able to access e-mail services and, depending on the specific VANS provider, other services such as hosting and virtual private networks (VPNs).

In essence, then, VANS providers in South Africa are the fundamental intermediaries allowing widespread access to the Internet and related services for businesses and consumers.

3.1.1 Applying for a VANS licence

Regulations regarding the procedure to be followed in an application for a VANS licence were promulgated by the Minister of Communications on 19 May 2004[42]. Application to ICASA must be made on the prescribed forms[43], setting out the business and contact details of the applicant, a general description of the service and technical aspects of the service, and the general geographical area in which the proposed service will operate[44]. In addition certified copies of type-approval certificates issued by ICASA in respect of telecommunications equipment to be used must accompany the application[45]. There are also requirements in respect of employment equity[46].

While concerns have been raised about licensing requirements and fees acting as a barrier to entry into the market of SME service providers,[47] it is submitted that the fees applicable are not onerous and that the application procedure is relatively straightforward. The fact that there are

---

[40] set out in the Ruling in the Telkom complaint against IS, para 4
[41] Thornton, Kristsos & De Villiers, "Telecommunications legislation as barriers to e-commerce" in in Cyberlaw II, ed Buys, Van Schaik Publishers 2004 p258
[42] Government Gazette 26371 notice 837, "Regulations relating to the manner in which application for Value-Added Network Service (VANS) licences are to be made" made in terms of section 96 of the Telecommunications Act; available from http://www.icasa.org.za/Repository/resources/Forms/1-25519-10%20Com.pdf (last visited 15 Sept 2004)
[43] Regulations (supra note 12) ss1(1); application form available from http://www.icasa.org.za/Repository/resources/Forms/VANSapplication.doc (last visited 15 Sept 2004)
[44] Regulations (supra note 12) ss1(2)-(5)
[45] Regulations (supra note 12) ss1(6)
[46] Regulations (supra note 12) s2
[47] Thornton, Kristsos & De Villiers, "Telecommunications legislation as barriers to e-commerce" in in Cyberlaw II, ed Buys, Van Schaik Publishers 2004 p258

currently hundreds if not thousands of unlicensed providers of internet services is more likely attributable to government policy and ignorance of licensing requirements.

3.1.2. Terms and conditions applicable to VANS licences

The general terms and conditions which will be applicable to all granted VANS licences include requirements to the effect that:

(a) the licensee provide the VANS by means of telecommunication facilities provided by an PSTS operator[48];
(b) the licensee is in general prohibited from disclosing any information about its customer which is obtained in the course of providing the VANS or use such information for any purpose other than in the performance of its obligations to clients, unless required to do so in order to comply with (a) above[49];
(c) information may, however, be disclosed to a third party to the extent that such disclosure may be required for the recovery of debts, auditing the books of the Licensee, litigation (potential, threatened or actual) and where requested by ICASA;[50]
(d) the licensee must clearly distinguish between VANS and other network services for which it is charging its customer and make this information available to ICASA upon request;[51]
(e) the licensee must establish "efficient procedures" for customer assistance and the satisfaction of customer complaints[52]; and
(f) the licensee must keep its financial records for a minimum of five years[53].

A VANS licence is valid for 10 years from the date of issue[54]. Applications for renewal of a VANS licence in accordance with section 49 of the Telecommunications Act must be made at least three months prior to the expiry date of the existing licence[55] – if no renewal application is received or granted then the licence will lapse[56]. VANS licences may be revoked by ICASA in accordance with the relevant provisions of the Telecommunications Act for any breach of the licence terms and conditions[57]. Licences may only be transferred in accordance with regulations promulgated under section 50 of the Telecommunications Act[58].

A full list of VANS licence holders can be obtained from the ICASA web site[59].

Most, if not all, ISPs, as traditionally perceived, are holders of VANS licences under section 40 of the Act. But there are a large number of "non-traditional" ISPs which provide Internet-related services which do hold a valid VANS licence, either through a failure to apply or through ignorance of the fact that they are providing a telecommunications service.

3.1.3. Equipment licensing

Under section 54 of the Telecommunications Act the prior approval of ICASA is required before a person may use, supply, sell, offer for sale, lease or hire any type of telecommunication equipment or facility. Telecommunications equipment or facilities utilised by ISPs must accordingly be type approved.

---

[48] s2(b)
[49] s2(c)
[50] ss2(c)(i)-(iv)
[51] ss2(d)
[52] ss2(e)
[53] ss2(f)
[54] s4.1
[55] s4.2
[56] s4.3
[57] s3
[58] s5
[59] at http://www.icasa.org.za/Repository/resources/Broadcasting/Licencing/Licensees/VANS-PTN%20LICENCE%20REGISTER%202004-04-06.xls (last updated 06.04.2004 & last visited 15 Sept 2004)

Application forms for type approval are available from the ICASA web site[60].

3.2. The Universal Service Fund (USF)

Under section 67 of the Telecommunications Act all licence-holders are required to contribute to the USF so as to contribute to the realising of the Act's objective of promoting universal and affordable provision of telecommunication services.[61]

3.3. Convergence

Convergence can be roughly defined as the trend towards different technology platforms being able to carry essentially identical services and the use of single, integrated devices by consumers for accessing, for example, telephone, data and television services. South Africa has produced a draft Convergence Bill which is likely to be published in final form later this year.

Technology convergence will offer huge opportunities for the development of new value added services and the anticipated legislation may well reclassify VANS as application and content service providers[62]. It is likely that the final passage of convergence legislation will be delayed by recent moves to liberalise regulation of telecommunications provision in South Africa.

3.4. Telecommunications liberalisation - a few comments

On 2 September 2004 the Minister of Communications announced far-reaching measures to provide a more competitive telecommunications industry in South Africa[63,64.] The three policy shifts directly applicable to VANS are set out below.

As of 1 February 2005:

- value added network services may carry voice using any protocol;
- value added network services may also be provided by means of telecommunications facilities other than those provided by Telkom and the Second National Operator or any of them; and,
- a person who provides a value added network service shall be entitled to cede or assign the right to use, or to sublet or part with control or otherwise dispose of the telecommunications facilities used for the provision of the value added network service.[65]

This means that the restrictive conditions relating to use of the PSTS and the prohibition of the resale of capacity currently applicable to VANS licence-holders will fall away[66].

While it is beyond the scope of this paper to delve into the implications of the above announcements, it seems certain that the implementation of these steps will result in there being far greater opportunities for VANS licence-holders to compete with Telkom. The full effect of policy liberalisation will take some time to become clear and there is likely to be a period of at least 2 years during which time the industry will see a rush of new entrants and ICASA will be hard-pressed to properly regulate conduct and issues such as termination costs and

---

[60] http://www.icasa.org.za/Default.aspx?page=1506 (last visited 22 Sept 04)
[61] see in this regard the web site of the USA – www.usa.org.za (last visited 25 Sept 04) http://www.ispa.org.za/downloads/ispa_sub_359.doc (last visited 22 Sept 2004)
[62] Alhadeff et al p244
[63] POLICY ANNOUNCEMENT BY THE MINISTER OF COMMUNICATIONS, DR IVY MATSEPE-CASABURRI found at http://www.doc.gov.za/Press_Stmnt_02Sep_2004.htm (last visited 22 Sept 04)
[64] the policy announcements are also aimed at allowing South Africa to meet its obligations under World Trade Organisation (WTO) rulings to which it is a signatory; see further Thornton *et al* at pp266-7
[65] and see General notice on the Policy determination of dates in terms of the Telecommunications Act, [Act No. 103 of 1996]found at http://www.doc.gov.za/images/Policy_deter_030904.pdf (last visited 22 Sept 04)
[66] see para 3.1.2. above

interconnection. It would seem that the Department of Communications will in future place responsibility for telecommunications in South Africa squarely in the hands of ICASA[67].

The relaxation of the prohibition on VoIP– transmitting voice calls as data packets using Internet Protocol – is likely to be one of the more difficult areas to regulate due to the simple fact that VoIP is vastly less expensive than traditional voice services. While the latter are distance-dependent and charged for accordingly, the former requires only a local call to a VANS provider after which the voice packet is transmitted over the VANS network[68]. At present there are only a handful of operators, other than Telkom, who have the capacity and expertise to provide carrier-grade VoIP over the so-called last-mile of connectivity, but the opportunity presented will be too good to ignore.

The fixing of a date for the legal provision of VoIP will relieve VANS licence-holders of the obligation to ensure that their customers do not use their services to provide VoIP. Due to the fact that there is no practical distinction between voice and data and that it is accordingly technically very difficult to prevent VOIP from being carried, VANS operators have relied on contractual prohibitions without means of enforcement, the need for which will, in most cases, fall away shortly.

4. ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 of 2002

The ECT Act can be regarded as the pioneering piece of South African legislation with respect to legal regulation of electronic communications and commerce. While the Act applies to ISPs in general as it does to other entities, the specific provisions relating to ISPs are fundamentally important in creating legal certainty and an enabling environment within which ISPs may function as intermediaries.

Although it is perhaps misleading to speak of legislated “obligations” of ISPs under the ECT Act there are a number of liability and self- and co-regulation issues which may arise through the applicability of the Act.

4.1. The Chapter XI framework for limiting the liability of service providers

The South African government has recognised that the fundamental role of ISPs as intermediaries in the provision and availability of Internet services to the public needs to be protected against the “huge”[69] potential for delictual and criminal liability under the provisions of existing statutory and common law in South Africa.

The primary civil or delictual liability risks to ISPs in this regard are liability as a contributory infringer of intellectual property and liability as a publisher of defamatory material. Without deviating into the detail of such risks, it is sufficient to state that, while there is a great deal of confusion both in South Africa and other major jurisdictions as to these risks, ISPs would be ill-advised to ignore them[70].

---

[67] Vecchiatio, P Regulator “has telecoms market in its hands” article on ITWeb, 20 September 2004 (available at www.itweb.co.za last visited 20 Sept 2004)
[68] Alhadeff et al p237
[69] Proposed IRB Guidelines (see full citation below) Part 1, para 1.1.
[70] for a discussion of the liability of ISPs prior to the enactment of the ECT Act see Buys (ed) Cyberlaw I at pp37-67 (copyright infringement) and pp337-341(defamation)

The enactment of Chapter XI of the ECT Act was an attempt to control this threat to the efficient functioning of Internet services in SA – it seeks to "provide protection to responsible ISPS" that meet certain minimum criteria broadly described in the Act and to be further refined by the Minister of Communications[71].

The basic structure of Chapter XI is to set out a number of common and activity-specific preconditions which, if complied with, will have the effect of shielding ISPs from claims that could be brought against them for classes of activities usually conducted by ISPs. These "safe harbour" provisions are substantially the same as the corresponding enactments in the US and EU.

The common[72] conditions for eligibility are that:

(a) The service provider must be a member of a representative body recognised by the Minister of Communications[73]. Recognition by the Minister is premised upon it being shown to his or her satisfaction that:
    a. Members of the body are subject to a code of conduct;
    b. Membership is subject to adequate criteria;
    c. The code of conduct requires continued adherence to adequate standards of conduct;
    d. The body is capable of monitoring and enforcing its code of conduct adequately[74].
(b) The ISP must have adopted and implemented the official code of conduct of the relevant representative body[75].

Once an ISP has adopted, implemented and is continuing to observe the code of conduct of a recognised industry body of which it is a member it will be exempt from liability if it further complies with the provisions relating to "conduit activities" which ISPs typically undertake as intermediaries – caching, hosting, search engine services and, more generally, where the ISP acts as a mere conduit.

This approach implicitly recognises the value of classifying ISPs according to the different functions they typically perform.

Take-down provisions and procedures, an integral element of the Chapter XI framework, will be discussed separately below.

4.1.1. Mere conduit

An ISP will be able to raise the statutory defence that it acted as a "mere conduit" in providing access to or for information systems or transmitting, routing or storing data via an information system under its control if it can show that it did not initiate the transmission, modify data contained in it or select the addressee and that it performed its functions in an automatic and technical manner without the selection of data[76]. The defence extends to claims based on the "automatic, intermediate and transient storage" of data transmitted by the ISP if this is done for no longer than is reasonably necessary, is done only to facilitate transmission and in a way that only anticipated recipients will be able to ordinarily access it[77].

[71] Proposed IRB Guidelines (see full citation below) Part 1, para 1.1.
[72] in the sense that all ISPs must comply with these irrespective of the kind of service provided
[73] ECT Act s72(a)
[74] ECT Act s71(2)(a)-(d)
[75] ECT Act s72(b)
[76] ECT Act s73(1)
[77] ECT Act s73(2)

This provision is broadly similar to that found in the United States Online Copyright Infringement Liability Limitation Act (OCILLA)[78] – Title II of the Digital Millennium Copyright Act (DMCA) of 1998[79] – and the European Union E-Commerce Directive[80]. The ECT Act provision differs from the E-Commerce Directive only insofar as the Act also requires that the ISP provide access services in an automatic, technical manner without selecting the data.

4.1.2. Caching

ISPs will be protected against liability for the "automatic, intermediate and temporary" storage of data via an information system under its control at the request of a third party provided

(a) the purpose of such storage must be for the provision of a more effective service to other recipients of the data;
(b) the data is not modified;
(c) the caching is undertaken in compliance with industry standards;
(d) there is no interference with the use of caching technology to get information on the use of the cached data;
(e) the specified take-down procedure is observed.[81]

4.1.3. Hosting

Hosting involves an ISP renting out space on a server which it owns and controls to a user who is able to post content to this space, for example by posting a message on a bulleting board or putting up a web page.

In general an ISP will not be liable for any unlawful or infringing activity arising out of a web-hosting service provided that

(a) it lacks actual knowledge of the infringing material;
(b) it is not aware of any facts which would indicate the infringing nature of a subscriber's activities; and
(c) it expeditiously disables access to or removes the infringing material upon receipt of a statutory take-down notice by its designated agent[82].

ISPs which perform a hosting function are in addition required to designate an agent to act on their behalf in the receipt of notifications of infringement. The name, address, phone number and e-mail address of the designated agent must be provided through the service of the ISP including web sites where the agent's details must be accessible to the public[83]. In South Africa a number of medium and large ISPs have designated the Internet Service Providers Association (ISPA) as their agent for this purpose.

4.1.4. Information location tools

Chapter XI also offers safe harbour to ISPs which provide search engine services wherefrom a recipient of the service may be provided with links to pages containing unlawful content or activities. Where an ISP operates a search engine, directory or index which lists links to third party web sites the ISP will not be liable for any unlawful content or infringing activities situated on any of the third party web sites, provided

(a) it lacks actual knowledge of the unlawful content or infringing activities on the web site to which a link is provided;
(b) it is not aware of facts which would serve to indicate the unlawful or infringing nature of the web site linked to;

---

[78] s512(a) can be found at http://thomas.loc.gov/cgi-bin/query/F?c105:2:./temp/~c105mLO18y:e34043:: (last visited 4 Sept 2004)
[79] can be found at http://thomas.loc.gov/cgi-bin/query/D?c105:2:./temp/~c105mLO18y::
[80] Art 12 found at http://europa.eu.int/comm/internal_market/en/ecommerce/index.htm
[81] ECT Act s74
[82] ECT Act s75(1)
[83] ECT Act s75(2)

(c) it does not receive any commercial or financial benefit directly attributable to the unlawful or infringing activity; and
(d) it either removes the link or disables access to it within a reasonable time after being informed of the unlawful or infringing activity.[84]

From (d) above it is possible to argue that an ISP may be obliged to remove or disable access to a link or reference to a web page which allegedly contains infringing material merely upon being informed thereof and without a take-down notification being received by the ISP. As a complainant would under such a scenario usually be in a position to be able to serve a take-down notification on the infringing page and the ISP hosting it, and as the possibility of substantial damages or even liability for wrongfully disabling or removing a link would be negligible, it is submitted that ISPs should respond positively to information received. This could be done by asking the complainant to submit a take-down notification or by disabling and removing the link or reference. In either case, it is submitted, they would fall within the safe harbour.

In all of the above scenarios, other than with regard to information location tools, an ISP may, notwithstanding the specific provisions of Chapter XI, be ordered by a competent court to terminate or prevent unlawful activity in terms of any other law[85].

4.1.5. ISP Obligations arising from membership of an Industry Representative Body (IRB)

The Department of Communications has recently released a Notice inviting comment on Proposed Guidelines for Recognition of Industry Representative Bodies in terms of Chapter XI of the Electronic Communications and Transactions Act, 2002[86]. Comments on the notice must be submitted by 8 October 2004.

The Proposed Guidelines for Recognition of IRB's in terms of Chapter XI of the ECT Act ("the Proposed IRB Guidelines") contain a Best Practice Code of Conduct[87], Checklist of Adequate Criteria[88] and a section on Monitoring and Enforcement[89].

4.1.5.1. Status of the Proposed IRB Guidelines

The Chapter XI schema follows the approach almost universally adopted in other jurisdictions, namely to place "the emphasis for control on self-regulation by the industry rather than directly applicable legislation or government regulation and intervention"[90]. The only role of the government is to act as an overarching control charged with ensuring that IRBs and their members meet certain specified minimum requirements as set out in the proposed guidelines.

The minimum requirements are also set out in a Checklist of Adequate Criteria against which the Minister will evaluate the compliance of an applicant IRB and consequently recognise or decline to recognise the applicant.

It is open to debate whether the approach adopted actually constitutes self-regulation as can be observed in other ISP self-regulatory schemes. As an IRB will not be recognised other than through compliance with the minimum criteria it follows that ISPs that wish to take the benefits of recognition as such under Chapter XI will also have to so comply. The proposed guidelines contemplate self-regulation only insofar as the IRBs will be responsible for ongoing

[84] ECT Act s76
[85] see ECT Act ss 73(3), 74(2), 75(1)
[86] Government Gazette 26768, General Notice 1951, 8 September 2004. Available from www.doc.gov.za
[87] Proposed IRB Guidelines Part 1
[88] Proposed IRB Guidelines Part 2
[89] Proposed IRB Guidelines Part 3
[90] Proposed IRB Guidelines, Part 1, para 1.2

implementation (failing which their status may be under threat) and not insofar as the setting of actual standards is concerned.

It remains to be seen to what extent industry input will be incorporated into the final guidelines but, as set out elsewhere, industry participation will be inadequate given the gulf between the legal definitions and traditional perceptions of ISPs.

4.1.5.2. Principles underlying the proposed guidelines

The proposed guidelines list 13 principles on which they are based[91] – certain of which are discussed below.

It is important to note that the proposed guidelines specify only the minimum requirements that must be met by IRBs and their members – the guidelines themselves specify that compliance with the minimum standards "does not necessarily guarantee that conduct will be legal"[92]. The guidelines also set out what is considered to be international best practice and identifies these standards as what IRBs and their members should be striving to attain[93]. These are referred to as "preferred standards of conduct" and are not mandatory[94], although there may well be marketing collateral to be gained through compliance with the preferred standards.

A further element of the intended objective of the proposed guidelines is the protection of consumers and the public – it being the perceived responsibility of the Department of Communications (DOC) to act in the public interest in setting minimum levels of professional conduct for ISPs. The minimum requirements in this regard relate to the notice and take-down provisions in section 77 of the ECT Act while the preferred standards of conduct also incorporate observance of the consumer protection and privacy provisions set out in Chapters VII and VII of the Act respectively[95].

The standards specified in the proposed guidelines have been designed to observe the doctrines of functional equivalence and technological neutrality[96].

A further principle is that the standards to be observed by IRBs and their members should be "fair and not adversely affect the economic viability of ISPs"[97].

The guidelines distinguish between "illegal conduct or content" and "potentially harmful content". The former is defined to mean information which it is illegal or unlawful to create, possess, publish or copy or any conduct which is illegal or unlawful under South African statutory or common law[98]. The possession, provision or dissemination of "potentially harmful content", on the other hand, need not be illegal, but includes content or information which "describes, depicts, expresses or otherwise deals with matters such as sex, bestiality, pornography, exploitation of children, torture, horror, crime, cruelty, or violence in such a manner that the availability of the information is likely to be injurious to the public good or protected groups such as minors"[99]. This class of content also covers information or content which may incite violence, cruelty or hatred on the basis or racial or sexual discrimination, creed or religion or which may incite the commitment of any crime[100].

---

[91] Proposed IRB Guidelines, Part 1, para 2
[92] Proposed IRB Guidelines, Part 1, para 2.4
[93] Proposed IRB Guidelines, Part 1, para 1.2
[94] Proposed IRB Guidelines, Part 1, para 2.6
[95] Proposed IRB Guidelines, Part 1, para 2.7
[96] Proposed IRB Guidelines, Part 1, para 2.11
[97] Proposed IRB Guidelines, Part 1, para 2.12
[98] Proposed IRB Guidelines, Part 1, para 4 definitions
[99] Proposed IRB Guidelines, Part 1, para 4 definitions
[100] *ibid*

4.1.5.3. Minimum requirements for a Code of Conduct

The following discussion does not cover all of the minimum requirements under the proposed guidelines.

Standard terms and conditions

Members of IRBs must provide the standard terms of agreement applicable to service agreements entered into with clients prior to the commencement of any service agreement. Standard terms of agreement must be available from the member's web site[101]. These terms must include

(a) a commitment to legal and lawful conduct in the use of the services provided;
(b) a commitment to compliance with take-down notices served on the client including a provision to the effect that where a client disputes the legitimacy of a take-down notice it will nevertheless take-down the allegedly unlawful content until resolution of the dispute;
(c) an obligation on client's to place on their web sites a "prominent reference" to the complaints procedure of the of the IRB of which the service provider is a member;
(d) a "guarantee" on the part of the client that it will not knowingly create, display, publish or copy that infringes the copyright of another;[102]
(e) a statement that the ISP member has the right to itself take down any content which it considers illegal or which the client has refused to take down notwithstanding receipt of a take down notice[103];
(f) a statement that the ISP member has the right to terminate or suspend the services provided to the client if it does not comply with the above or any other "related contractual obligations"[104];
(g) an undertaking by the client that it will not send or promote the sending of spam[105]; and,
(h) a "guarantee" on the part of their clients that will not access, intercept or interfere with data without specific authorisation.[106]

Service levels

IRBs are obliged to publish a minimum service levels guideline from time to time and must be satisfied that the minimum service levels as stated in their members' standard terms of agreement are acceptable within the context of the nature of a particular members services and area of operation[107].

Content Control

The proposed guidelines reiterate that it is not expected of ISPs (which are members of an IRB) that they monitor content, rather that they cannot ignore potential or actual illegal or unlawful content or conduct[108]. There is an explicit statement that "[t]he content provider is primarily and directly responsible for contents provided"[109].

[101] Proposed IRB Guidelines, Part 1, para 5.2.1
[102] Proposed IRB Guidelines, Part 1, para 5.2.2(a)-(d)
[103] Proposed IRB Guidelines, Part 1, para 5.2.3
[104] Proposed IRB Guidelines, Part 1, para 5.2.4
[105] Proposed IRB Guidelines, Part 1, para 5.8.3
[106] Proposed IRB Guidelines, Part 1, para 5.10.2
[107] Proposed IRB Guidelines, Part 1, para 5.3.3
[108] Proposed IRB Guidelines, Part 1, para 5.4.2
[109] Proposed IRB Guidelines, Part 1, para 5.4.1

An interesting minimum standard relates to the fact that ISPs are prohibited from knowingly carrying, transmitting, caching, hosting or providing links to content that it knows or "reasonably suspects to be" unlawful or illegal[110]. With the lack of clarity surrounding copyright concerns and file-sharing on P2P networks the position may be adopted that caching of files to facilitate this service would breach the minimum standard of content control concerned.

Consumer protection

The standards in this regard include compliance with compulsory advertising standards and regulations[111] and commitments to integrity[112] and honest and fair dealing[113].

Privacy & Confidentiality

Members of an IRB are, *inter alia*, required to respect the confidentiality of client commercial information[114], e-mail and electronic messaging[115]. ISP members are also prohibited from dealing in or with the personal information of data subjects other than for "their own needs" or with the express prior permission of the data subject[116].

Spam protection

IRBs and their members are required to play a proactive role with regard to unsolicited commercial communications by taking "reasonable steps" to ensure that their networks are not used for the sending of spam or related activities[117]. ISP members are also obliged to refrain from sending or promoting the sending of spam[118].

Although it is not explicitly stated the reference to spam must be read subject to the spam provisions in the ECT Act and commercial communications which comply with the requirements of the Act[119] would presumably be acceptable.

The proposed guidelines contain a definition of spam as meaning "unsolicited commercial communications (as defined in the ECT Act)". As there is no definition of "spam" or "unsolicited commercial communications" in the ECT Act it is submitted that this definition should distinguish between unsolicited commercial communications which are lawful in the sense that they comply with the ECT Act requirements[120] and those that are not.

"Reasonable steps" to ensure that an ISP network is not used for spamming could include the use of filters, providing clients with spamming software so that they can elect to minimise the amount of spam received[121], the implementation of effective privacy practices and security and client education. A prohibition on spamming and the promotion of spam should appear in the ISP's standard terms of agreement. An ISP should also be able to demonstrate compliance with any applicable industry standards.

A court considering whether reasonable steps have been taken would also, it is submitted, be prudent to bear in mind the massive technological and legal efforts already targeted at preventing

[110] Proposed IRB Guidelines, Part 1, para 5.4.3
[111] Proposed IRB Guidelines, Part 1, para 5..5.3
[112] Proposed IRB Guidelines, Part 1, para 5.5.2
[113] Proposed IRB Guidelines, Part 1, para 5.5.1
[114] Proposed IRB Guidelines, Part 1, para 5.6.4
[115] Proposed IRB Guidelines, Part 1, para 5.6.3
[116] Proposed IRB Guidelines, Part 1, para 5.6.2
[117] Proposed IRB Guidelines, Part 1, para 5.8.1
[118] *ibid*
[119] set out in section 45 of the ECT Act
[120] see ECT Act ss45(1) and 45(4)
[121] this is one of the preferred standards of conduct - see Proposed IRB Guidelines, Part 1, para 6.8

spam and the fact that, despite these, spam remains a massive problem in electronic communications.

It is in any event in the direct interests of ISPs to take all such cost-effective steps against spam as are available. Spam has a direct economic cost, endangers servers and creates user dissatisfaction. Given the fact of pecuniary damage, and wishing away the ever present problems of jurisdiction, it is submitted that there is a strong argument that ISPs would enjoy *locus standi* in a suit against an identified spammer.

Protection of minors

ISP members must provide links to and information on procedures and software which filter or label content so as to facilitate control and monitoring of minor's access to potentially harmful conduct.[122]

Cybercrime

The security measures adopted by an ISP must be such that it can be said to have taken "all reasonable measures to prevent unauthorised access to, interception of, or interference with any data"[123]. It is submitted that ISPs would be well advised to seek certification under a recognised security standard such as SANS 17799 so as to be able to demonstrate the taking of all reasonable measures.

Disciplinary procedure

The powers afforded IRBs to regulate the conduct of their members are fairly substantial. IRBs will be expected to have a Complaints Procedure and Disciplinary Code which is binding on members[124] and will be entitled to receive and investigate complaints by customers of members[125]. Members will be obliged to cooperate with the IRB in the resolution of a complaint[126].

IRBs are also empowered to investigate compliance with their codes and institute disciplinary proceedings of their own initiative[127].

If a member is found to have breached the applicable code of conduct after the holding of a hearing under the Disciplinary Code[128] then the IRB may sanction the member through the issuing of a take-down notice (if relevant) together with either a reprimand, conditional suspension, expulsion and/or the publication of the details of the transgressor and transgression and the reporting of the transgression to the relevant law enforcement agency[129].

It is submitted that there is sufficient heft in the potential sanctions so as to constitute a compelling reason for compliance with the IRB code of conduct (and accordingly the rules set down by government). Expulsion from an IRB will lead to an ISP being at risk of civil liability for its hosting, caching and other services.

Monitoring of compliance

---

[122] Proposed IRB Guidelines, Part 1, para 5.9.2 & 5.9.3
[123] Proposed IRB Guidelines, Part 1, para 5.10.1
[124] Proposed IRB Guidelines, Part 1, para 5.12.1
[125] Proposed IRB Guidelines, Part 1, para 5.12.2
[126] Proposed IRB Guidelines, Part 1, para 5.12.3
[127] Proposed IRB Guidelines, Part 1, para 5.13.3
[128] Proposed IRB Guidelines, Part 1, para 5.12.5
[129] Proposed IRB Guidelines, Part 1, para 5.12.6(a)-(f)

ISP members must submit an annual report confirming compliance with the IRB code of conduct to the relevant IRB.

Informational requirements

The logo signifying membership of an IRB must be prominently displayed by members along with a reference to the applicable code of conduct and contact details in respect of complaint procedures and take-down notices[130]. The use of hyperlinks to achieve this should, it is submitted, comply with the "incorporation by reference" provisions of the ECT Act[131].

The full contact details of the member ISP, covering the contact and indentifying information required to be laid out under Chapter VII of the ECT Act[132], must be set out on its web site.

4.1.5.4. Preferred requirements for a Code of Conduct

Due to the non-mandatory nature of the preferred requirements an in-depth discussion thereof is beyond the scope of this paper. Under these standards ISP members will be required to comply fully with the consumer protection and privacy provisions contained in Chapter VII and Chapter VIII respectively of the ECT Act and further to obtain a commitment from their clients that they will also so comply[133]. There are also provisions in respect of ISP conduct in the registration and availability of domain names[134] and the provision of redirection facilities to former clients who have changed ISPs[135].

The augmented requirements of the preferred standards of conduct should be reviewed and adopted where possible. Many of these standards cast an obligation on a member ISP to ensure a level of acceptable conduct from their clients and in this respect they will function as regulatory bodies in respect of their client bases.

4.1.6. Notice and take-down

The procedure in respect of take-down notifications is laid out in section 77 of the ECT Act. The essence of the procedure is that a complainant who believes that an ISP is providing services which infringe his or her rights must issue a notification containing, inter alia, identification of the allegedly unlawful material or activity[136], to the ISP or its designated agent. Subject to certain exceptions an ISP will then be obliged to remove the allegedly unlawful material. ISPs are protected against liability for damages for wrongful take-down in respect of a party whose material has been removed or to which access has been disabled on the strength of a take-down notification issued by an ISP[137].

It can be seen from the discussion of the minimum standards of conduct above that, as regards take-down procedures that there are a number of standard terms which ISPs must include in the agreement for the provision of services which are concluded with their clients. There will accordingly be a contractual obligation on clients to comply with take-down notices issued to them notwithstanding any dispute as to the legitimacy of a notice. A failure on the part of the client to observe a take-down notice will have the result that the relevant ISP will itself remove material or disable access while having the option to terminate the service contract and claim damages, if any. The refusal of a client to perform properly in response to a take-down notification will also be an aggravating factor in any civil or criminal action which may ensue.

---

[130] Proposed IRB Guidelines, Part 1, para 5.14.1
[131] section 11(3) ECT Act
[132] section 43(1) ECT Act
[133] Proposed IRB Guidelines, Part 1, para 6.2(a) & (b)
[134] Proposed IRB Guidelines, Part 1, paras 6.3.3. to 6.3.5
[135] Proposed IRB Guidelines, Part 1, para 6.3.6
[136] full requirements for a take-down notification are set out in s77(1)(a)-(h)
[137] section 77(3) ECT Act

The minimum standards of conduct also stipulate that an ISP must make it clear to its clients that it reserves the right to, of its own initiative, take down content which it regards as being illegal. In this case the ISP must, when it first becomes aware of the presence of illegal conduct or content, serve a take down notice on the relevant client and/or suspend or terminate the client's services and/or report the conduct or conduct to an enforcement agency, "whichever actions are the most appropriate".[138] Any action taken and the reasons for which it was taken must be reported to the relevant IRB within a reasonable period of time.

Copies or records of all complaints, take down notices and content removed must be kept for three years unless, in the case of content, possession thereof is illegal, in which case it must be forwarded to the relevant enforcement agency[139].

Member ISPs are required to comply with all take down notices received unless they are "obviously frivolous, unreasonable, vexatious or in bad faith".[140]

It is interesting to note that qualifiers used in respect of the time periods within which an ISP is required to remove material or disable access thereto differ across the different ISP activities contemplated by Chapter XI. Where a take-down notification is received in respect of cached material it must be simply removed or disabled[141], while hosted material must be "expeditiously" removed or disabled[142] and links or references to infringing data must be disabled or removed "within a reasonable time" after receiving information that it infringes the rights of another[143]. This distinction seemingly relates to the perceptions of potential harm which can result from the respective activities.

The clear advantage to ISPs of working within this framework is that it removes uncertainty and risk. If an ISP acts in compliance with the above then it cannot, under any circumstances, be held liable for disabling access or removing material pursuant to a take-down notice which contains a material misrepresentation.

The Act provides that the mere fact of the provision of access to the Internet by an ISP and the provision by it of a system that is used for transmitting third party information does not of itself render the ISP liable for contributory infringements in respect of the activities of the third party.

The notice and take-down provisions found in OCILLA contain an interesting additional element to the ECT Act approach – the "put back" procedure. OCILLA holds that where an ISP has received proper notice and as a result blocks access to allegedly infringing material, the ISP must take reasonable steps to inform the subscriber that provided the blocked content of the fact that access has been blocked. The affected subscriber then has an opportunity to file a counter-notification with the ISP advising that the removal or blocking is due to a mistake or misidentification. If this counter-notification complies with the requirements set out then the ISP must provide a copy to the original notifier and it will be obliged to to replace the allegedly infringing content or enable access to it unless the notifier informs it that a court action seeking to restrain the alleged infringement has been filed.

[138] Proposed IRB Guidelines, Part 1, para 5.4.7
[139] Proposed IRB Guidelines, Part 1, para 5.4.8
[140] Proposed IRB Guidelines, Part 1, para 5.4.5 in which case it must refer it to the relevant IRB and notify the complainant (see para 5.11.2)
[141] ECT Act s74(e)
[142] ECT Act s75(c)
[143] ECT Act s76(d)

4.1.7. No general obligation to monitor

Finally, and importantly, the Act specifically states that ISPs are not under any general obligation to monitor data which is stored or transmitted by them[144], nor are they obliged to actively seek facts or circumstances which may indicate unlawful activity[145].

Interestingly, however, the Act does contemplate that the Minister may, subject to the privacy provisions set out in the Bill of Rights, prescribe procedures for ISPs to "inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service"[146]. Procedures may also be prescribed by the Minister for the communication to the competent authorities, at their request, of information which will allow the identification of a recipient of an ISP service[147].

The absence of a general obligation on ISPs to monitor the content or conduct of their clients is one of the principles underlying the Proposed IRB Guidelines, but is balanced against recognition of the fact that "responsible ISPs" should not be allowed to simply ignore illegal conduct or content within their sphere of operation or control of which they are aware[148].

4.2. Conclusions

It is submitted that the position under the ECT Act brings much desired certainty to the position of ISPs with regard to civil liability for the acts and omissions of its subscribers. The procedure to be followed is relatively simple and the safeguards built into the notice and take-down procedure will largely serve to prevent abuse and a corresponding chilling effect on freedom of speech and commercial activity, although there will still no doubt be some misuse of the provisions due to the fact that the balance of convenience for ISPs will almost always be in favour of restricting or disabling access.

The author's recent experience in representing the owner of the domain name www.telkomsucks.co.za against a claim for R5 million rand in respect of trademark infringement and defamation is instructive as regards such potential misuse. In this matter Telkom elected to approach the web site owner directly by way of letter of demand setting out the reasons it believed the domain name (as opposed to the actual content of the site) to be unlawful and damaging to its rights and demanding that use of the name cease immediately. Subsequent events would seem to indicate that Telkom could only have been aware that the alleged causes of action were completely without foundation.

In following this course of action Telkom was either unaware of, or chose not to utilise, the notice and take-down provisions in the ECT Act. It is submitted that it would have been a far more effective avenue for Telkom to target the ISP hosting the site with a take-down notice. The ISP, a member of the Internet Service Providers Association (ISPA) and subject to the ISPA Code of Conduct, in exercising its discretion as to whether to disable access to the site, would consider the fact that complying with the dictates of the take-down notice would, subject to all other preconditions as they exist being met, obviate the possibility of any liability for wrongful take-down. Any confusion in the law, as it currently stands, would, it is submitted, have acted to the benefit of Telkom.

The net outcome of this approach is that the site, including content, would have been "taken down" and the site owner would thereafter have to initiate action against Telkom for the reinstatement of access to the web site.

---

[144] ECT Act s78(1)(a); a similar provision is to be found in the EU E-Commerce Directive
[145] ECT Act s78(1)(b)
[146] ECT Act s78(2)(a)
[147] ECT Act s78(2)(b)
[148] Proposed IRB Guidelines, Part 1, para 2.9

(Of course it may have been the position that Telkom, being aware of the dubious nature of its claim, did not wish to make the required statement that the information in the take-down notice was to its knowledge true and correct. It is submitted, however, that liability for wrongful take-down rests on a misrepresentation of the facts and not a misrepresentation of the law[149]).

The broad approach of Chapter XI with regard to ISP liability is similar to that adopted in the United States and the European Union. It is submitted that SA ISPs should consider implementing of their own accord a procedure based on the "put-back" provisions of OCILLA discussed above.

Nel[150] believes that the structure of Chapter XI is to be welcomed and that the "notice and take-down" provisions offer "a realistic and practical solution to protect the rights of all the relevant parties"[151].

5. REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF COMMUNICATION-RELATED INFORMATION ACT 70 OF 2002 ("RICA")

RICA, signed into law on 30 December 2002, but yet to be proclaimed in the Government Gazette, introduces significant legally-derived operational obligations for entities acting as Internet service providers in South Africa.

The Act, expected to come into operation in the near future[152], is one of the results of a comprehensive review of the law on interception and monitoring of communications commenced by the South African Law Commission in 1998[153]. At the time the SALC was of the opinion that the primary reason for reviewing the old Act was to "ensure that the emphasis in the new Act is on crime"[154]. The departure point and nature of RICA were subsequently impacted on by the 11 September 2001 attacks in the United States and the ensuing extension, in a great number of jurisdictions around the world, of traditional wiretapping[155] laws to new technologies and the introduction of augmented powers to law enforcement agencies.

Another contributing influence to the final form of RICA was the international treaty obligation occasioned by South Africa's signature of the Council of Europe Convention on Cybercrime ("the Cybercrime Convention")[156]. The primary objective of the Cybercrime Convention is to pursue a common criminal policy aimed at the protection of society against cybercrime through international cooperation and the adoption by signatories of appropriate legislation, and to this

---

[149] ECT Act s77(2)
[150] Nel, S "Freedom of expression and the Internet" in Cyberlaw: The Law of the Internet in South Africa II, ed Buys, R Van Schaik Publishers 2004
[151] Nel *supra* para 2.3.2.2 page 207
[152] Anonymous source in the Department of Communications; cf the publication of draft directives under s30 – discussed below – which seem to indicate that the Act will be in force within the next six months; see also presentation at iWeek 2004 Conference by Jayesh Nana (Technical Committee Chair, Office of Interception Centres) & Edmund Baloyi (Legal Affairs, Department of Communications)
[153] SALC, Project 105, November 1998
[154] SALC Discussion Paper 78, Project 105, Review of Security Legislation: The Interception and Monitoring Act 27 of 1992, p10
[155] usually targeted at fixed telephone services
[156] available from http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm (last visited 26 Sept 2004) and see http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG (last visited 26 Sept 2004)

end it contains provisions relating to the interception of communications[157]. The Cybercrime Convention came into force on 1 July 2004 and has 30 signatories of which 8 parties have implemented legislation to carry its provisions into effect. [158]

As a result of these and other factors, including, no doubt, the perceived desirability of government access to the immense information holdings contained in electronic communications, RICA bears little resemblance to its predecessor, the Interception and Monitoring Act 127 of 1992. The 1992 Act was enacted largely to increase privacy protections and can, in this sense, be seen as both conforming to the Bill of Rights in the Interim Constitution, existing in draft form at the time, and as a reaction to apartheid surveillance practices[159].

RICA, on the other hand, while containing a strong prohibition on the unlawful interception of communications, contains numerous provisions which can be seen, justifiably or otherwise, as eroding constitutionally-guaranteed privacy rights. Both RICA and the 1992 Act are products of the prevailing times and the gulf between the objectives and provisions of the two Acts represents the complexity of the challenge to the law in keeping pace with technological innovation and world events.

Given global and local events legislation of a similar nature to RICA is likely to become more prevalent and invasive. Legitimate concerns surrounding the use of the Internet for criminal and terrorist ends and for the storage of evidence of crime and terror are unlikely to abate in the near to middle term.

In the very real sense that RICA represents a balancing act between the right to privacy of communications and the interests of the State (and its citizens) in fighting crime and promoting national security, it is telecommunications service providers (TSPs) that represent the fulcrum upon which this balance is to be achieved. The importance of TSPs in realising the objectives of RICA once again calls into question the role which ISPs play and the tension that exists between ISPs as custodians of private information on behalf of their clients and ISPs as agents of the State.

5.1. Classes of information held by ISPs

By way of creating a context for the ensuing discussion, it is worthwhile to briefly consider the classes of information which are typically held by ISPs and which may be identified by law enforcement agencies as potentially beneficial in fighting crime and ensuring national security. Kerr and Gilbert[160] identify three basic classes of information held by ISPs in respect of their clients.

a. Customer Name and Address and Local Service Provider Identification (CAN/LSPID)

This is the basic level of information held by ISPs regarding their clients and is analogous to information contained in a telephone directory.

In a typical scenario a law enforcement agency would approach an online service provider such as Hotmail and request the details of a local service provider which has provided connectivity to a particular e-mail user. The law enforcement agency can then approach the local service provider and request the customer data required, including the customer's name, address and billing information.

---

[157] particularly the procedural provisions in Section2;
[158] see http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG for an updated list (last visited 26 Sept 2004)
[159] see S v Naidoo and Another [1998] 1 All SA 189 @ 213
[160] see fn 1

Due to the public nature of this information there can be virtually no expectation of privacy with regard to CAN/LSPID information on the part of wither the local service provider or its clients.

b. Traffic data

The Convention on Cybercrime defines traffic data as:

"any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."[161]

The corresponding term under RICA is "communication-related information".

Under this definition traffic data can be seen to comprise the details of the route travelled by an electronic communication as it travels from one user to another. It could also include the information contained in the sender, recipient and subject fields as also the title of any attachment(s) to the communication. In respect of web browsing traffic data would probably include a list of the web sites visited by a user and the amount of time which the user spent at each site.

A great deal of derivative information can be obtained from an examination of traffic or communication-related data. The nature of web sites visited may give a clear indication of a particular user's browsing habits being illegal (e.g. child pornography) or of potential interest to law enforcement (e.g. sites known to be frequented by terrorist groups).

Traffic data is generally regarded as constituting the second level of information held by ISPs. Due to the fact that an inspection of traffic data may reveal a great deal about a user's online practices it is intuitive that user's have a higher level of expectation of privacy than they do in CAN/LSPID data.

c. Content data

Content data such as the actual text component of an e-mail is the third class of information held by ISPs and users' would typically have a high level of expectation of privacy in this information.

d. Classification difficulties

As can be seen from the above, the real importance of the classification of user information held by ISPs relates to the levels of privacy which users' would expect with regard to each class. The differing expectations of privacy in turn dictate the ease with which law enforcement agencies should be able to obtain access to the user data. Where, for example, a law enforcement agency seeks access to content data this would generally have to be pre-authorised by a judge or magistrate to ensure that the breach of privacy entailed is justified.

Kerr and Gilbert express strong reservations about this categorisation of information held by ISPs on the basis that it is often extremely difficult to determine whether a particular piece of data falls within one or the other. They hold the view that the distinction between traffic and content data, in particular, can be fraught with difficulty, giving the example of a user entering a search query into a search engine. On one hand entering search criteria can be regarded as a necessary step in accessing content while another perspective is that the content of the search criteria entered will inevitably give a clear idea of the content of a user's web browsing itself.

A further difficulty with this three-fold classification is that data mining can be used to combine distinct pieces of information held for distinct purposes in a manner which may well reveal

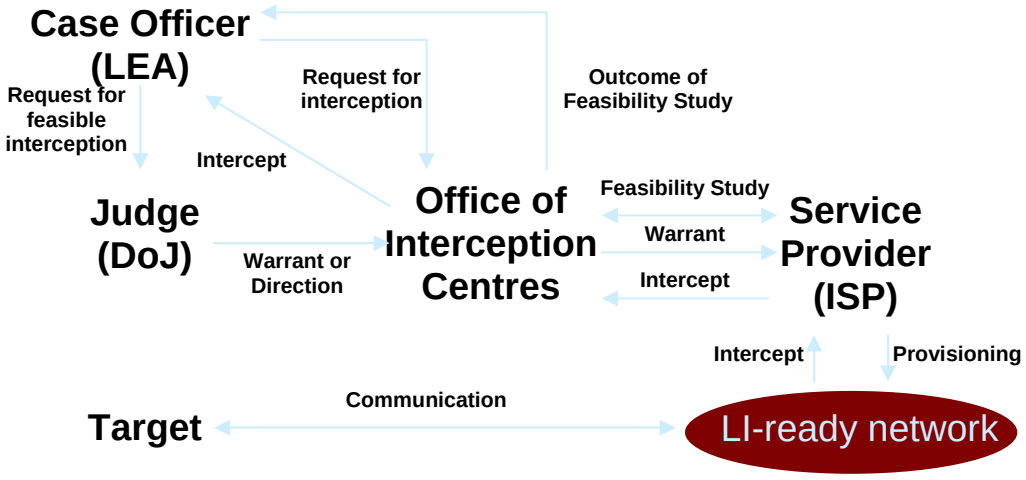
[161] Article 1(d)

content. In this way distinct sets of information which are seemingly innocuous in isolation can become extremely significant when combined. The combination of different sets of data can be seen as illegitimate in the sense that the final outcome fails to respect the original rationale underpinning the collection of each individual piece of data.

The difficulties in classifying data held by ISPs holds serious implications for the role which ISPs are expected to play, both as custodians of personal information and as legislated players in crime prevention and national security. Where an interception direction is issued it is the ISP which will have to implement the infrastructure necessary to monitor and intercept the different classes of information and determine whether particular information should be regarded as traffic or content data.

5.2. Overview of obligations imposed by RICA

The following diagram[162] illustrates the proposed inter-relationship between Law Enforcement Agencies (LEAs), the Office of Interception Centres (OIC) and ISPs with regard to Lawful Interceptions (LIs).



ISPs which fail to comply with obligations under RICA face fines and, if they are the holder of a telecommunications service licence, the possibility of revocation of such licence for repeated infringements.

5.2.1. General prohibition

ISPs are, as with all other persons subject to the Act, bound to observe the general prohibition on the unlawful interception of communications contained in RICA[163]. The general prohibition and the exceptions[164] thereto will apply to ISPs as they apply to other entities – they will, for example, have to act lawfully where monitoring the communications of their own employees.

[162] taken from presentation at iWeek 2004 Conference by Jayesh Nana (Technical Committee Chair, Office of Interception Centres) & Edmund Baloyi (Legal Affairs, Department of Communications), available from http://www.ispa.org.za/iweek/presentations/Jayesh.Nana.ppt (last visited 12 September 2004)
[163] RICA s2
[164] RICA ss3-9

5.2.2. Specific prohibition on information disclosure by ISP or employee

Over and above the general prohibition there is a specific prohibition on ISPs and their employees intentionally providing or attempting to provide real-time or archived communication-related information to any person other than the relevant customer unless authorised to do so under the Act[165]. Specific authorisations are laid out in section 13-15 and relate to release of information to a third party where required under an interception direction[166], through customer authorisation[167] and where the information is otherwise obtainable under any other law[168].

A failure to observe this prohibition by either the ISP or an employee is made an offence by section 50(1) of the Act. The maximum penalty where an ISP which is a juristic entity is convicted under this section is a fine of R5 million[169]. Employees[170] and ISPs which are natural persons[171] can be sentenced to a maximum fine of R2 million or to imprisonment for a period not exceeding ten years.

This provision will necessitate the implementation of stringent personnel security and confidentiality measures. Personnel will need to be trained as to what constitutes communication-related information and the circumstances under which it may be lawfully released.

Customer authorisation is required to be in writing and, although RICA is silent on this, it is submitted that it would be prudent for an ISP to retain this authorisation in its client file for at least the duration of its contractual relationship with the relevant customer.

5.2.3. Collection, verification and retention of customer information

Under RICA ISPs are required to comply with “know your customer” obligations such as typically found on banks in money-laundering legislation[172]. It is clear from RICA that an ISP must collect and verify clear identifying information in respect of natural[173] and juristic persons[174] prior to entering into a service contract with them. The required information includes a certified copy of the identity document of the potential client or the natural person representing it. The information collected must be stored and maintained to reflect any changes thereto.

ISPs will therefore, subsequent to the promulgation of RICA, have to amend the manner in which service contracts are entered into and this will have substantial consequences for the convenience with which such contracts can be finalised. Where it is now possible and commonplace for contracts for the provision of Internet access to be entered into entirely online it appears that this will no longer be possible (or at least inconvenient).

This is essentially the Customer Name and Address and Local Service Provider Identification (CAN/LSPID) information referred to above, and the lower level of privacy expectation is reflected in the fact that ISPs are required to “immediately comply”[175] with a written request from a party who is an applicant for an interception direction and requires information for the purpose of making such application. In particular an ISP will be required to confirm that the subject of the

[165] RICA s12
[166] RICA s13
[167] RICA s14
[168] RICA s15
[169] RICA s51(3)(b)(i)(bb)
[170] RICA s51(3)(b)(ii)
[171] RICA s51(3)(b)(i)(aa)
[172] RICA s39
[173] the information to be collected is set out in RICA s39(1)(a)
[174] the information to be collected is set out in RICA s39(1)(b)
[175] when the request concerns one of their customers – RICA s39(4)

request is its customer and provide the subject's telephone or other contact numbers together with a photocopy of the relevant identity document[176].

There is no provision as to the length of time for which this information must be retained. In the absence of applicable and compulsory data protection legislation which might impose an obligation to destroy or anonymise obsolete data it is submitted that it would be prudent for ISPs to retain such data for the duration of the service contract and for at least one year thereafter.

A failure to collect, verify or store customer information as required is an offence subject to the same penalties as set out for an unlawful disclosure of information by an ISP or one of its employees[177].

ISPA has queried the need for consumers to provide identification details before accessing the Internet and point out that the practical benefit of such provisions is questionable. It is relatively simple to dial around the system through an international phone call to a country without identification requirements.

In the event that Internet Cafés and the like are to be regarded as ISPs for the purposes of RICA (in that the provide access to the Internet) then they too would ostensibly be required to collect the necessary information and documentation prior to allowing a customer to use their facilities. It is difficult to see how this would be workable.

5.2.4. Assistance to be provided

Section 28 of RICA sets out the broad framework under which ISPs will be required to assist law enforcement authorities in the execution of directions under the Act. This framework will be canvassed in detail below.

5.2.5. Prohibition on provision of a service which cannot be intercepted

Chapter 5 of RICA relates to the interception capability of TSPs. It contains a direct prohibition on the provision by a TSP of any telecommunication service which is not capable of being intercepted[178] or which cannot store communication-related information[179]. These requirements have now been significantly fleshed out through the release of a Directive for Internet Service Providers in terms of section 30(7)(a) read with section 30(2) of RICA[180] ("the Directive").

The definition of an ISP for the purposes of the Act is as it is found in RICA[181]. There is also an explicit further statement that the Directive "applies to and is binding on all ISPs irrespective of whether they have been issued with a licence under Chapter 5 of the Telecommunications Act or not"[182].

The broad thrust of the Directive is that all ISPs must ensure, at their own cost, that their networks are surveillance enabled and capable of storing communication-related information for the required periods

[176] RICA s39(3)
[177] RICA s50(3)(iii) read with s50(3)(b)
[178] RICA s30(1)(a)
[179] RICA s30(1)(b)
[180] available from the homepage of the Department of Communications web site – www.doc.gov.za
[181] Directive Part 1 para 1 definitions
[182] Directive Part 1 para 2

5.3. The Section 30(7)(a) Directive for Internet Service Providers

Under section 30(7)(a) of RICA the Cabinet member responsible for communications must, within two months of the commencement of the Act and after consultation with affected Ministries, ICASA and the affected category of telecommunication service providers, issue a directive under section 30(2)(a) determining:

(a) the manner in which TSPs must provide an interception and storage capability;
(b) the security, technical and functional requirements of facilities to be acquired by TSPs so as to enable interception of indirect communications and storage of communication-related information; and
(c) the classes of communication-related information which must be stored and the periods for which it must be stored.[183]

Similar draft Directives have been issued to Fixed Line Operators and Mobile Cellular Operators.

5.3.1. Interception of indirect communications

An indirect communication is defined in RICA as meaning:

> "the transfer of information, including a message or any part of a message, whether-
> (a) in the form of-
> a. speech. music or other sounds:
> b. data:
> c. text;
> d. visual images, whether animated or not;
> e. signals; or
> f. 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 telecommunication system;"

ISPs, whether as licensed VANS providers or not, provide services for the transmission of indirect communications.

The Directive sets out in some detail the type of interception capability required and the manner in which ISPs are to conduct an interception.

The provision of a telecommunications service capable of being monitored entails the provision of a service in respect of which the packets of all indirect communications can be duplicated a routed to the Interception Centre through the application of software and/or hardware[184]. In the event that it is not possible for an ISP to duplicate and route the packets constituting an indirect communication, the ISP is nevertheless required to duplicate and route to the Interception Centre any other available results of the interception[185].

ISPs must ensure that applied software and/or hardware must be able to identify the targeted communication on the basis of its IP address, RADIUS login information[186] and/or e-mail

[183] RICA s30(2)(a)(i) – (iii)
[184] Directive para 4.2 (a) & (b)
[185] Directive para 7.14
[186] The RADIUS Attribute 8 (Framed-IP-Address) in Access Requests feature makes it possible for a network access server (NAS) to provide the RADIUS server with a hint of the user IP address in advance of user authentication. An application can be run on the RADIUS server to use this hint and build a table (map) of user names and addresses. Using the mapping information, service applications can begin preparing user login information to have available upon successful user authentication. See for example

address. The Directive contemplates that law enforcement agencies may need to use identifying characteristics in order to determine what traffic needs to be intercepted. Where this is justified by the applicant for the direction and is necessary given the special properties of a given telecommunications system, ISPs must be able to ensure that traffic can be clearly[187] identified, without unreasonable effort[188], on the basis of

(a) address information – physical or postal address;
(b) user name;
(c) subscriber name (where this may differ from the user name);
(d) e-mail address; and
(e) IP address and the time stamp indicating when the IP address was assigned.[189]

The content of an indirect communication routed to the Interception Centre must include both incoming and outgoing content[190].

The scope of the interception capability must extend to all "interception targets"[191], defined as customers whose indirect communications are to be intercepted or whose real-time communication-related information or archived communication-related information is to be routed by the ISP to the Interception Centre or provided to a law enforcement agency[192].

Given that ISPs have no way of knowing in advance exactly which of their customers may become an interception target, this effectively means that they have to be able to monitor and store information in respect of their entire customer database.

Where a direction or request has been properly received an affected ISP must ensure that it is able to it is able to intercept the entire content of an indirect communication associated with a target identity (i.e. an identity associated with an interception subject) for the period specified and to record checksum information on the results of the interception[193].

An important rider to the above, particularly given concerns about the constitutionality of RICA in the light of the rights to privacy contained in the Bill of Rights, is that, where technically feasible, ISPs must attempt to provide the results of an interception to the Interception Centre of law enforcement agency without disclosing any information which does not fall within the scope of the interception direction.

This is potentially problematic. Firstly, the ability to protect the privacy of a customer in respect of information which is not required to be disclosed is left up to the technical capabilities of the ISP – the ability to differentiate between disclosable and non-disclosable information is not mandatory. This ability may become a marketing differentiator for ISPs in the future – where a customer has privacy concerns they may well elect to utilise the services of an ISP which undertakes to protect the privacy of that customer's information to the maximum possible extent.

Secondly, where this technical capacity does exist, in the absence of extremely explicit information identifying the precise information to be disclosed under a direction or request it will be within the discretion of an ISP to decide what information is to be disclosed under a direction or request and what information is not required to be disclosed. ISPs are not judicially qualified to make these decisions and, initially and perhaps until a body of experience of dealing with directions and requests under RICA has been developed, it is likely that ISPs will err on the side

---

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121dc/121dc3/ip_hint.htm (last visited 9 September 2004)

[187] Directive para 7.16
[188] Directive para 7.16
[189] Directive para 7.15
[190] Directive para 7.9
[191] Directive para 4.3
[192] Directive para 1 definitions
[193] Directive para 4.2 (a) & (b)

of caution. The implication is that the right to privacy of its customers may be unjustifiably infringed through the disclosure of information not required under a legalistic interpretation of the terms of an interception direction or request.

Furthermore there do not appear to be safeguards against abuse by ISPs, particularly in the forthcoming period during which RICA and the Directive will be in force without there being a balancing set of rules embodied in privacy legislation.

5.3.1.1. Unchanged state of service

A further technical requirement in the implementation of an interception capability is that ISPs must conduct an interception in such a way that no telecommunicating parties[194] or unauthorised parties[195] will be able to detect any difference between communications which are or are not the subject of an interception. The operation of the target service and the quality of such service must not be altered or degraded as a result of the implementation of an interception direction or request[196].

The need for these provisions flows from the fact that any indication available to a targeted user that his or her communications are being intercepted will obviously prejudice the effectiveness of the interception.

The Directive also seeks to ensure that interception activities implemented by ISPs do not detrimentally affect the operation and quality of any other telecommunications service provided by an ISP[197]. While it may be technically feasible to maintain the operation and quality of other services, this will only happen to the detriment of consumers on to whom the cost burden will be passed.

5.3.1.2. Security requirements for Interception

There are a number of controls dealing with various security requirements surrounding the implementation of an interception capability and the ongoing implementation of specific interceptions.

Non-disclosure of related information

The Directive prohibits the release to unauthorised persons of information relating to the manner in which implementation measures are implemented[198] or to any target identities and target services to which interception is being applied[199]. ISPs are obliged to ensure that they have an appropriate non-disclosure agreement in place with any third party that has undertaken the implementation of an interception capability on behalf of a specific ISP[200]. In addition ISPs are required to take such steps as are available to ensure that the configuration of their telecommunications systems is such that interception measures can be implemented and operated with no or minimum third party involvement[201].

It is suggested that this element of non-disclosure should also be extended to the staff of the ISP and to any other third parties which may have access to information concerning the implementation of that ISP's interception capability. Staff and other third parties will need to be

[194] Directive para 5.2
[195] Directive para 5.1
[196] Directive para 5.3 read with para 5.4
[197] Directive para 5.3 read with para 5.4
[198] Directive para 6.1
[199] Directive para 6.2
[200] Directive para 6.3
[201] Directive para 7.11

effectively trained and bound to ensure that none of the information listed in the preceding paragraph is disclosed other than in accordance with the Act and Directive.

The Directive mandates that ISPs shall undertake the necessary technical arrangements "with due care exercised in operating telecommunications installations"[202], and with particular respect to:

(a) protecting information on individual target identities and the number of target identities subject to interception which are or were subject to interception together with the periods during which interception measures were active[203];
(b) keeping the number of staff involved in implementing and operating interception measures to a minimum[204];
(c) ensuring that interception measures are carried out in distinct operating rooms which are only accessible to authorised personnel[205];
(d) clearly specifying and delimiting the functions and responsibilities of personnel so as to assist in the maintenance of third-party telecommunications privacy[206];
(e) ensuring that the handover interface between the ISP and the Interception Centre is available[207] and that "all necessary measures" have been taken to protect this interface against misuse[208] or access by unauthorised persons[209];
(f) ensuring that the handover interface supports the use of encryption, authentication, integrity checking or other confidentiality measures and co-operating with applicants or the Interception Centre where required to implement such measures[210] - the cost of such measures where requested will be borne by the Interception Centre[211];
(g) ensuring that the results of an interception are only handed to the Interception Centre as set out in the direction or request for such interception and only once the ISP has furnished proof of its authority to send such results to the handover interface and received proof from the Interception Centre to the effect that it is entitled to receive such results[212];
(h) authentication and proof of authentication when utilizing the handover interface will be in accordance with national laws and regulations[213] and, where switched lines to the Interception Centre are used proof of authentication must be provided for each call set-up[214] [215];
(i) that misuse of the technical functions enabling the interception and which are integrated into the technical installation must be able to be traced or prevented through the recording of any activation or application of such functions in respect of any target identity[216], including
    a. the target identities of the target service or target services;
    b. the beginning and end of the activation or application of the interception measure;

[202] Directive para 6.4
[203] Directive para 6.4(a)
[204] Directive para 6.4(b)
[205] Directive para 6.4(c)
[206] Directive para 6.4(c)
[207] Directive para 6.4(d)
[208] Directive para 6.4(f)
[209] Directive para 6.4(e)
[210] Directive para 6.4(k)
[211] Directive para 6.4.(j)
[212] Directive para 6.4(g)
[213] Directive para 6.4(h)
[214] Directive para 6.4(i)
[215] and see the Draft Accreditation Authority Regulations as published in the Government Gazette No. 26602 on the 30th July 2004. *(Notice No. 1537 of 2004);* available from www.doc.gov.za
[216] Directive para 6.4(l)

c. the Interception Centre to which information resulting from the interception measure is routed;
d. an authenticator which identifies the operating staff and shows the date and time of input;
e. a reference to the direction or request.[217]

The records collected when complying with (i) above must be secure and only accessible to specific nominated staff within the ISP[218].

It should be apparent from the above that ISPs will be required to invest heavily in security. It is submitted that, given these and other obligations and potential liabilities, compliance with and certification under an appropriate security standard should be a *sine qua non* for medium and large ISPs at the very least.

5.3.1.3. Technical and functional requirements in respect of interceptions

Section 7 of the Directive contains provisions relating to the interaction between ISPs and Interception Centres and the clear identification of the application of specific interception measures.

As regards the configuration of the handover interface between an ISP and an Interception Centre, the Directive requires that such configuration must ensure that the results of interceptions are provided[219] for the duration of the interception measure[220], and that the quality of service of the telecommunications traffic provided to the handover interface is at least equivalent to that offered to the target service[221].

The configuration of the handover interface must allow routing to the Interception Centre of the results of an interception under industry standard transmission paths, protocols and coding principles[222].

In order to avoid mis-identification of results of interception measures every interception target must be uniquely associated with a single instance of the handover interface, which may be accomplished through the use of separate channels or "unique interception identifiers"[223]. There must be a unique correlation between an indirect communication and communication-related information which is relevant to it[224].

When routing intercepted indirect communications to an Interception Centre ISPs must utilise an industry standard format[225] allowing transmission via a "secure tunnel" [226] over circuit or packet switched connections[227].

ISPs must inform the Interception Centre of the following in respect of an interception measure:
(a) activation;
(b) deactivation;
(c) changes to the interception measure;

[217] Directive para 6.4(l)(i)-(v)
[218] Directive para 6.5
[219] Directive para 7.2
[220] Directive para 7.1
[221] Directive para 7.3
[222] Directive para 7.4
[223] Directive para 7.5
[224] Directive para 7.6
[225] Directive para 7.7
[226] see para 1 definitions: "secure tunnel" means an encrypted and authenticated IP communication channel established using the most recently published versions of the IP Secure (IPSec), Transport Layer Security (TLS), or Secure Socket Layer (SSL) protocols
[227] Directive para 7.8

(d) any temporary unavailability of the interception measure due to failure or fault on the ISP's side of the link;
(e) any temporary unavailability of the interception measure due to software and/or hardware failure suffered by ISP equipment which supports the interception measure[228].

5.3.1.4. Co-operation between ISPs or between ISPs and TSPs

The Directive provides that ISPs that utilise a telecommunication system operated by another TSP then, where required, the two parties must co-operate in implementing and maintaining an interception measure[229]. Where an ISP needs to involve another TSP in providing an interception then the ISP, as the recipient of the relevant direction or request , must ensure that only so much information about operational activities as is strictly necessary in order to effect the interception is given to the TSP[230].

5.3.1.5. Multiple interceptions

Multiple interceptions can take place either through a direction specifying more than one interception target or through more than one separate direction applying to a single interception target.

With regard to the former ISPs must ensure that the indirect communications of multiple customers can be simultaneously intercepted at any given time and the results routed to the Interception Centre[231].

ISPs are obliged to ensure that more than a single interception measure can be taken in respect of one and the same interception target and service.[232] The Directive requires that ISPs must take "reasonable precautions" to safeguard the identities of the various law enforcement agencies involved and to protect the confidentiality of their investigations. Presumably this means that an ISP cannot reveal to an applicant for a direction the fact that an interception measure in respect of the interception target and service is already in place.

Where multiple law enforcement agencies are involved, the practical implementation of this provision could be nigh on farcical – given the requirements relating to confidentiality and dedicated staff canvassed above ISPs could be stretched in terms of manpower and finances where they have the misfortune to have as a customer someone who has raised the curiosity of many.

It should be noted that, where a target identity participates in a multi-party or multi-way communications (such as a multicast), an ISP must route and duplicate the relevant packets to the Interception Centre only where and for as long as the target participates in the multi-party communication[233].

[228] Directive paras 7.10(a)-(e)
[229] Directive para 7.12
[230] Directive paras 7.13(a) & (b)
[231] Directive para 7.20
[232] Directive para 7.17
[233] Directive para 4.8 read with para 4.7

5.3.2. Routing, provision and storing of real-time communication-related information

There is a general prohibition on ISPs providing a telecommunication service "in respect of which all real-time communication-related information can be securely stored, retrieved and duplicated" for routing to the Interception Centre or provision to a law enforcement agency[234].

"Real-time communication-related information" is defined in RICA to mean "communication-related information which is immediately available to a telecommunication service provider-

(a) before, during, or for a period of 90 days after, the transmission of an indirect communication; and
(b) in a manner that allows the communication-related information to be associated with the indirect communication to which it relates."[235]

5.3.2.1. General requirements

Real-time communication-related information relating to an interception direction must be immediately stored by ISPs for a period of not less than 90 days[236]. ISPs must take steps to ensure[237] that this information is "immediately retrievable" within this period[238]. Storage must be in a format which is in accordance with the relevant direction and which allows "extraction of the relevant requested information only, in a readable, intelligible and understandable format".[239]

The standard of care to be observed by ISPs with regard to such stored information is high – the Directive explicitly states that ISPs must ensure that real-time communication-related information is not accidentally or deliberately deleted[240].

Where an ISP is unable, for whatever reason, to immediately route real-time communication-related information to the Interception Centre then the ISP must either buffer such information until it can be routed or provide the information in an alternative manner[241].

5.3.2.2. Recording and content of real-time communication-related material

Where an ISP has received a real-time communication-related direction together with an interception direction or request in respect of the same target identity, or a real-time communication-related direction that requires information to be made available as it is received, the ISP must, subject to and in accordance with any instructions contained in the direction or request, provide such information from the time when an interception target first establishes a connection to the ISP and for the duration of that target's connection so established[242].

Section 9 of the Directive continues to specify the classes of real-time communication-related information which an ISP must be able to provide in respect of

(a) Network Access Systems[243];
(b) Servers wholly owned and administered by the ISP[244];
    a. E-mail servers (SMTP, POP and/or IMAP logs)[245];
    b. File upload and download servers (FTP logs)[246];

---

[234] Directive para 8.1
[235] RICA s1 definitions
[236] Directive para 8.2
[237] Directive para 10.8
[238] Directive para 8.3
[239] Directive para 8.7
[240] Directive para 8.8
[241] Directive para 8.10
[242] Directive para 9.1
[243] Directive para 9.2 "Network Access Systems" are described as "access logs specific to authentication and authorisation servers used to control access to IP routers and/or network access servers".
[244] Directive para 9.3
[245] Directive para 9.3(a)

c. Web servers (HTTP logs)[247];
d. Usenet (NNTP logs)[248];
e. Internet Relay Chat (IRC logs)[249];
f. Information available in the records of the ISP in any other protocol used in sending, downloading, uploading or accessing any communication[250].

The information classes to be provided varies according to each of the categories listed above but will generally include the date and time of connection of the client; user name and IP addresses. A full list of real-time communication-related information by category is set out in the Directive.

5.3.2.3. Security requirements

The security requirements relating to the storage of real-time communication-related information are largely identical to those applicable to interceptions and can generally be applied *mutatis mutandis*.

Additional requirements in respect of this class of information relate to the actual storage thereof. An ISP must ensure the integrity of the information at the time at which it is stored. It is also obliged to take steps to ensure the physical, environmental and logical security of all stored real-time communication-related information.

5.3.2.4. Technical and functional requirements

An ISP must provide all "relevant requested" real-time communication-related information in a readable, intelligible and understandable format and in accordance with the applicable direction[251]. As is the case regarding interceptions the handover interface must be configured to allow the routing of information provided, over a secure tunnel[252], using industry standard transmission paths, protocols and coding principles[253] and the routing format must be industry standard[254]. Whenever real-time communication-related information is provided each instance of provision must be uniquely identifiable[255].

ISPs are obliged to inform the Interception Centre in the event of there being any change to the storage system, measures and functionality employed in the storage of real-time communication-related information. They must also disclose any temporary unavailability of stored information.[256]

The configuration of an ISPs storage system must allow storage, maintenance, extraction, processing and transmitting or provision of real-time communication-related with no or minimum involvement by third parties[257].

The provisions with regard to co-operation with other TSPs are, *mutatis mutandis*, identical to those in relation to interceptions, as are those regarding multiple interceptions. As opposed to the corresponding requirement with regard to interceptions the Directive envisages that the impossibility of providing or routing real-time communication-related information will only exist in "exceptional cases". Any remaining information must nevertheless be provided.[258]

---

[246] Directive para 9.3(b)
[247] Directive para 9.3(c)
[248] Directive para 9.3(d)
[249] Directive para 9.3(e)
[250] Directive para 9.3(f)
[251] Directive para 11.1
[252] Directive para 11.5
[253] Directive para 11.2
[254] Directive para 11.4
[255] Directive para 11.3
[256] Directive para 11.6
[257] Directive para 11.7
[258] Directive para 11.10

Storage devices and media must clearly index or identify the information stored upon them to facilitate efficient retrieval[259].

5.3.3. Routing, provision and storing of archived communication-related information

A telecommunication service offered by an ISP must be capable of storing, retrieving and duplicating all archived communication-related information for routing to the Interception Centre or provision to a law enforcement agency[260].

"Archived communication-related information" is defined in RICA as meaning any communication-related information in the possession of a telecommunication service provider and which is being stored by that telecommunication service provider in terms of section 30(1)(b) for the period determined in a directive referred to in section 30(2)(a) beginning on the first day immediately following the expiration of a period of 90 days after the date of the transmission of the indirect communication to which that communication-related information relates."[261]

5.3.3.1. General requirements

In transferring communication-related information to an archived storage facility ISPs must ensure that no data is lost[262] and that the information is not transferred until the expiry of 90 days from the date on which the relevant indirect communication was recorded[263]. The integrity of transferred data must be preserved.[264]

The provisions of the Directive with regard to the time period for archived communication-information must be stored appear contradictory. ISPs are required to have the capability to provide specified information in respect of both Network Access Systems and E-mail servers. Section 12.2 of the Directive provides that "information pertaining to Network Access Systems only" must be stored and available (or retrievable[265]) for a period of five years[266]. A later provision, however, holds ISPs must "be able to provide" information obtained in respect of both Network Access Systems and E-mail servers for the same period[267].

Provisions in respect of routing and duplication and storage format are identical to those applicable to real-time communication-related information.

5.3.3.2. Security requirements

The security requirements in respect of archived communication-related information are identical to those in respect of real-time communication-related information. ISPs must ensure the integrity of the information when it is stored, during transfer to any storage media or device and for the entire period set our in "paragraph 17".[268]

5.3.3.3. Technical and functional requirements

These requirements are identical to those in respect of real-time communication-related information.

---

[259] Directive para 11.11
[260] Directive para 12.1
[261] RICA s1 definitions
[262] Directive para 12.6(a)
[263] Directive para 12.6(b)
[264] Directive para 12.6(c)
[265] Directive para 12.3
[266] as stipulated in Part 5 para 16
[267] Directive para 13.1
[268] Directive para 14.6 – the reference to paragraph 17 is probably intended to point towards paragraph 16 and, for the sake of consistency should probably read "for a period stipulated in Part 5 of this Directive"

5.3.4. Part 6 – Detailed requirements

Part 6 of the Directive sets out detailed requirements and requires that "as far as possible" ISPs must adopt specifications relevant to their networks from a choice of specified documents. Any deviations and option choices from specifications set out in these documents must be communicated to and agreed upon by the Interception Centre before implementation.[269]

Three documents are specified which are described as follows:

(a) Specification of LI requirements for ISPs providing an Internet Access service directly to end-users;
(b) Technical interface for mediation and handing over of intercepted IP telephony traffic to an IC;
(c) Technical interface for the mediation and handing over of intercepted e-mails to an IC.

5.4. Retention of communication-related information – data retention vs. data preservation

Data retention is of itself one of the single most important issues facing the both the South African and global ISP industries. A recent proposal for a European Council Framework Decision on data retention calling for significant obligations on ISPs for the collection, storage and retrieval of data has caused dismay amongst European ISP associations[270].

Data retention is seen by many as an extreme solution, the need for which has not been justified. In the United States, for example, where there is no mandatory data retention, there have been no difficulties with US law enforcement agencies successfully obtaining the data which they require. The experience of many European ISPs has been that very few, if any, requests for retrieval of retained data are received from law enforcement authorities.[271]

Mandatory data retention has been likened to a requirement that the Post Office retain a record of the sender, recipient and routing of all items sent through the postal service. But, given that an electronic communication will generally travel between separate networks and pass through other networks while doing so, the analogy grossly understates the problem. Sheer volume aside there is the problem of multiple retention of records – where multiplicities of ISPs store an identical piece of data in multiple locations.

Retrieval of data under a legislated data retention regime is likely to become increasingly ineffective in direct relationship to the amount of data retained, as is the security surrounding extended data holdings. The more difficult it is to retrieve data the longer the response time to the request from the relevant law enforcement agency.

A legal difficulty with data retention, particularly for European ISPs, is the conflict between data retention and data protection requirements, such as the EU Directive on Data Privacy for Electronic Communications[272]. Data protection requirements, which mandate ISPs to delete or anonymise customer data, are clearly at odds with blanket retention rules, placing ISPs in an untenable position. The drafters of South Africa's future data protection legislation will have to weigh this tension very carefully indeed and the ISP industry will need to communicate a very clear position in this regard.

---

[269] Directive para 20.2.
[270] see EUROISPA Response to the Consultation Document on Traffic Data Retention (available from www.euroispa.org, last visited 22 September 2004) and EUROISPA & USISPA position on the impact of data retention laws on the fight against cybercrime, 30 September 2002 (available from www.euroispa.org, last visited 22 September 2004)
[271] ibid
[272] Directive 2002/58/EC

It is argued that mandatory retention will put as great deal of personal information at risk of misuse or accidental disclosure. Even in countries where the State has undertaken to cover the cost of data retention and retrieval ISPs are faced with the almost insurmountable obligation of ensuring that the integrity and security of the huge amount of data collected.

An alternative means of ensuring the availability of evidence for the purposes of crime prevention and national security is data preservation, an approach which has been approved by the Council of Europe and the G-8. The G-8 has defined data preservation as the specific preservation of historical data so as to prevent its deletion on the basis of a lawful request from a competent authority based on the facts of a specific case and pending issuance of a lawful demand from a competent authority[273].

Under this definition ISPs are not required to collect and retain data on a prospective basis and they are further not obliged to generate any data that is not routinely required for lawful business practices. The conflict between data retention and data protection can be obviated through the use of preservation orders under which ISPs will be authorised to preserve specific data on individual targets beyond deletion dates imposed by data retention laws.

EuroISPA and USISPA have accordingly urged that countries considering mandatory data retention should conduct a comprehensive cost-benefit analysis of the impact of retention, and should contrast the results of this analysis against a similar exercise focusing on data preservation[274].

To the author's knowledge no such investigation has taken place in South Africa and there is no provision for data preservation of this form in RICA[275]. While South Africa currently lacks a detailed data protection regime, there is a strong argument that the availability of data preservation as a more proportionate response to crime prevention imperatives would be more in line with the Constitutional guarantees in respect of privacy and privacy of communications.

Indeed, when the perhaps inevitable constitutional challenges to RICA do arise, it is submitted that an argument that mandatory data protection is unconstitutional in that it is an unjustifiable limitation on the right to privacy of communications will be of exaggerated force and effect if it can be shown that data preservation, a less intrusive means, more efficiently achieves the same ends as data retention.

Recent developments, discussed below, do, however, offer hope that the South African government has recognised the potential folly of obliging ISPs and others to retain data for lengthy periods.

5.5. Technical implications of RICA for ISPs

A comprehensive analysis of the technical challenges posed to ISPs through the need to comply with RICA is as far beyond the scope of this paper as it is beyond the competence of the author. Nevertheless there are certain issues which need to be alluded to.

It should firstly be noted that the nature of the challenge will differ across ISPs according to their size, service offerings, network structure and business evolution. Secondly, it is possible for ISPs to lease an interception and storage capability from either a larger ISP or other third party.

---

[273] EUROISPA & USISPA position on the impact of data retention laws on the fight against cybercrime, 30 September 2002 (available from www.euroispa.org, last visited 22 September 2004)
[274] *ibid*
[275] the Cybercrime Convention does contemplate preservation orders – articles 16 and 17

5.6. Financial implications of RICA for ISPs

It is evident from the above analysis that technical compliance with the Directive will raise serious challenges to ISPs, particularly those in the SME sector and non-traditional service providers. But experience in other jurisdictions has indicated that it is the financial rather than the technical implications which bear the potential to cause serious disruptions to the ISP industry.

As stated above, all costs of routing, as well as the costs of interception, monitoring, procurement of equipment and storage, are to be borne by ISPs. ISPs will also have to cover related costs such as those involved in training staff, having dedicated facilities, appointing administrative contacts and ensuring that they comply with security and privacy obligations.

The state will be responsible for the establishment of interception centres, which will be managed and control by a statutory body to be known as the Office for Interception Centres ("OIC"), which will be funded by the State. The OIC will bear the costs of establishing interception centres and of connecting to ISPs amongst others.

Estimating the volumes of data that would need to be retained on the basis of RICA and the Directive as they now stand is dependent on the services offered and subscription base of ISPs, but is likely to be hundreds of times that which is required today. While the common storage media currently used may not be overly costly, storage devices able to cater for the projected volumes of data have yet to be developed and the related costs will be prohibitive.[276]

Staff-related costs will also put undue strain on ISP budgets. The personnel charged with handling interception directions and requests will need to be thoroughly qualified and trained, and they will have to be able to adapt to technical changes made in the ISPs systems on a fairly regular basis.

Alhadeff *et al* opine that it is unfortunate that RICA does not take into account the European Union Mutual Legal Assistance (MLA) Convention and the international benchmarks set out therein[277]. As has been noted above South Africa is a signatory of the Cybercrime Convention (in pursuance of which much of RICA was enacted) but not to any of the other EU laws, particularly those of a countervailing or balancing nature – such as the Data Protection Directive – and those of a complementary nature – such as the MLA Convention. Article 21 of the MLA Convention requires that member countries bear the costs incurred by telecommunication operators in the course of executing interception and other directions.

In the United States more than USD500 million was paid to telecommunications companies as reimbursement for the costs of compliance with wiretaps, although nothing was paid to Internet service providers[278]. In Australia, where VANS are also required to develop and implement an interception capability at their own cost, the actual costs and burdens on ISPs have exceeded expectations, with the result that government was forced to implement substantial subsidies and exempt telecommunications carriers from the requirements for several years[279].

The Netherlands has also adopted a legislative framework for the real-time interception of e-mail and data without there being any facility for the reimbursement of ISPs. As is the case with RICA, intercepted data must be accompanied by call-related information and must be converted into a secure format before being transferred to the relevant law enforcement agency.

---

[276] see EUROISPA Response to the Consultation Document on Traffic Data Retention (available from www.euroispa.org, last visited 22 September 2004)
[277] Alhadeff *et al* at p242
[278] McCullagh, Declan "Internet surveillance: US practices" speech delivered at iWeek 2004 Conference, found at http://www.ispa.org.za/iweek/presentations/Declan.Mccullagh.ppt (last visited 24 Sept 2004)
[279] Alhadeff *et al* fn80 p248

The cost to the ISP industry of complying with these obligations has been estimated at EUR 30 million by the Association of Netherlands Internet Providers (NLIP)[280], who believe that 25% of the industry will not be able to afford the cost of compliance and that they will either go out of business or be forced to operate at a loss for some years to come[281].

In order to meet these concerns RICA makes provision for the establishment of the Internet Service Provider's Assistance Fund ("the Fund")[282]. This will be funded by contributions made as determined by the Minister by ISPs which have been exempted under section 46)(1)(a), and will be managed by the Office for Interception Centres (OIC).

Money in the Fund must be used for the purchasing or leasing of facilities and equipment to be used by the police in executing interception directions served on ISPs which have been exempted from the requirement to purchase such facilities and devices[283].

5.6.1. Exemptions

The Minister of Communications may, upon application and in consultation with the relevant Ministers, exempt any ISP from the requirement that it must, at its own cost, acquire, whether by purchasing or leasing, the facilities and devices to be stipulated in the finalised Directive promulgated under section 30(2)(a)[284]. Such exemption may be subject to conditions, which could include a requirement that the exempted ISP or class of ISPs pay an annual contribution determined by the Minister to the Internet Service Providers Assistance Fund established under section 38[285]. A certificate of exemption must be issued and this will be effective from the date of its publication in the Government Gazette[286] subsequent to approval by the National Assembly[287]. A certificate of exemption may be withdrawn or amended[288].

The granting of an exemption to an ISP does not absolve it of any other of its responsibilities under RICA. The practical effect of the exemption will be that, where a law enforcement agency requires the co-operation of an exempted ISP, it will be required to provide the necessary facilities and devices to execute an interception direction[289].

There is very little guidance in RICA as to what will constitute valid grounds for exemption, although the Act specifically makes mention of an ISP which "carries on such a small business that he or she cannot provide" the necessary facilities and devices at his or her own cost[290]. Mention is also made of exemptions which are in the public interest[291] and around which special circumstances may exist.[292]

It is possible and even likely that the exemption clause will be used to exempt SMEs for at least period of time in respecting of paying for their own interception capability. It may even be used to give the entire industry a period of grace. Exemptions in the public interest or motivated by special circumstances may include libraries, government departments, NGOs and educational institutions such as schools and universities.

---

[280][280] see further ww.nlip.nl (only available in Dutch, last visited 14 Sept 2004)
[281] Alhadeff et al p243
[282] RICA s38
[283] under RICA s46(1)(a) and s46(7)(b) see below
[284] RICA s46(1)(a)
[285] RICA s46(1)(b)
[286] RICA s46(3)
[287] RICA s46(4)
[288] RICA s46(5)
[289] RICA s46(7)
[290] RICA s46(2)(a)
[291] RICA s46(2)(c)
[292] RICA s46(2)(d)

In any event it is clear that the any party wishing to avail itself of the exemption will need to make application therefore, and that the approval of the application will take some time. Intelligent use of this exemption is a potential lifeline for many entities legally defined as ISPs.

5.7. Conclusion

The present status of RICA and the Section 30 Directive constitutes a real and direct threat to the ISP industry and to many other entities which may fall under RICA due to the ambiguity of the legal definition of ISPs. It remains to be seen how RICA and the Directive will be implemented but it seems certain that the technical and financial implications of compliance will threaten the continued economic viability of ISPs both big and small and that this will lead to a decrease in competition and an increase in the costs to consumer of Internet services.

RICA may even have the effect of severely distorting the competitive balance of the industry in that its financial effect will vary according to the size and network structure of each individual ISP.

Given that no Internet service which cannot be intercepted and monitored can be provided, it is even possible that ISPs may simply elect not to offer certain services so as to avoid the related compliance costs.

Applications for exemptions from parties, at an industry, group or individual level will offer some relief to many legally defined ISPs and the manner in which the Minister and the National Assembly regard such applications will be crucial to the effectiveness of RICA. A refusal to grant warranted exemptions will be disastrous to certain entities such as libraries and educational institutions. It will also have the effect of frustrating the crime-prevention objectives of RICA as entities unable to comply will not have an interception capability and will not be catered for by law enforcement agencies providing facilities and devices themselves.

Latest indications are that many of the financial realities posed by RICA are being appreciated by government. A representative of the Department of Communications[293] indicated in early September 2004 that the requirements in respect of the storage of real-time and archived communication-related information may be “scrapped” and that the focus of RICA will be exclusively on the interception of indirect communications. There is also movement to allow smaller ISPs to obtain assistance from larger ISPs or third parties.

Not having to store staggering amounts of data for lengthy periods will represent a huge cut in the compliance bill and, given the doubts raised about data retention, it is submitted that any move to do away with storage requirements is to be enthusiastically encouraged.

RICA is expected to be promulgated in the near future. Once RICA has come into force the Directive will be finalised and proclaimed within two months and ISPs will then have six months within which to either comply (through purchasing their own capability or making an arrangement with a larger ISP or third party to lease or otherwise obtain such capability) or successfully obtain an exemption.

While it is doubtful that the worst possible scenario for ISPs under RICA will be realised, the almost deafening silence from the industry and entities affected by the Act and their lack of input in the drafting process must be a continuing cause for concern.

[293] presentation at iWeek 2004 Conference by Jayesh Nana (Technical Committee Chair, Office of Interception Centres) & Edmund Baloyi (Legal Affairs, Department of Communications)

6. FILM & PUBLICATIONS AMENDMENT ACT (FPAA)

The Film & Publications Amendment Act of 2004, expected to be signed into law at the time of writing, amends the Film & Publications Act 65 of 1996 with specific regard to the prohibition of child pornography. As with RICA, the enactment of the FPAA was at least partly motivated by South Africa's obligations as a signatory to the Cybercrime Convention[294].

Due to the perceived role of the Internet as a facilitating factor in the distribution of child pornography, there are several provisions in the Amendment Act which are relevant to this discussion of ISPs.

The Act, insofar as it purports to impact on ISPs, is also an excellent example of legislation drafted without due consideration of the pre-existing legal context. The Amendment Act originates from the Department of Home Affairs. It is, with respect, not surprising to note that, the explicit objects of the act regarding Internet service providers notwithstanding, that the Department of Communications does not appear on the list of organisations or persons consulted in the drafting of the Amendment Act[295].

Child pornography is an almost universally accepted evil which prima facie justifies the most onerous intrusions on individual rights in combating it. As such it can be seen as an extreme case – the thin edge of the wedge – where law enforcement can claim a simplistic blanket justification in taking such steps as it may regard necessary to fight it. The concern for privacy advocates is that intrusions justified on the basis of combating child pornography all too easily find their way into other areas of Internet regulation.

Accordingly the issue of child pornography is an especially sensitive element of illegal conduct around which ISPs have a role to perform, one which they generally embraced. It is important to clearly distinguish between illegal content and potentially harmful content, i.e. content which is not per se illegal but which some may find offensive or which special groups such as children should be protected from.

In its submission to the portfolio committee, ISPA stated that it held the view that the object of the FPAA in fighting child pornography on the Internet through the regulation of ISPs is "somewhat of a misconception" for the reason that ISPs do not produce, distribute or offer child pornography on the Internet, nor do they directly control the content posted on web sites or Internet chat-rooms.

To the writer's mind this somewhat misses the point. The regulation of child pornography is the shared responsibility of governments (which must create clear, appropriate and consistent laws and seek international co-operation), law enforcement agencies (which must find ways to effect cross-border co-operation) and ISPs. ISPs, empowered by at least a degree of actual physical control, are crucial not only to effective regulation but also to the protection of others from exposure to child pornography. This is purely by dint of their intermediary status.

---

[294] Title 3 Article 9 reads:

"Article 9 – Offences related to child pornography

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a. producing child pornography for the purpose of its distribution through a computer system;
b. offering or making available child pornography through a computer system;
c. distributing or transmitting child pornography through a computer system;
d. procuring child pornography through a computer system for oneself or for another;
e. possessing child pornography in a computer system or on a computer-data storage medium"

[295] from Memorandum on the objects of the Films and Publications Amendment Act 2004, section 2

6.1. "Possession" and "distribution"

"Possession" under the FPAA is defined as including "keeping or storing [a film or publication] in or on a computer or computer system or computer data storage medium and also having custody, control or supervision on behalf of another person"[296].

"Distribute" as defined includes the failure to take reasonable steps to prevent access to a film or publication to a person under the age of 18 years.

This represents a clear difficulty to ISPs. Will an ISP acting as an access provider or as a mere conduit be considered as a distributor simply for unknowingly providing access to a prohibited film? Will cached content be sufficient for possession? Is a web hosting company the custodian, controller or supervisor of child pornography uploaded by one of their clients without its knowledge?

The ISPA submission[297] raised the fact that provisions regarding exemptions for ISPs in this regard have already been enacted in the ECT Act. The "mere conduit" provisions[298] contained in Chapter XI of the ECT Act hold that, assuming compliance with the conditions for eligibility[299], a service provider will not be liable for, *inter alia*, providing access where it

(a) does not initiate the transmission;
(b) does not select the addressee;
(c) performs the functions in an automatic, technical manner without selection of the data; and
(d) does not modify the data contained in the transmission[300].

Liability is also excluded for transient storage and hosting under the conditions set out in the ECT Act[301], which would effectively deal with problems around the definition of "possession" under the FPAA. It is also important to remember that, the above provisions notwithstanding, it is still open to a competent court to order an ISP to terminate or prevent unlawful activity in terms of any other law.

It would appear logical that the entire framework for the exemption of ISPs from liability as engineered in Chapter XI of the ECT Act should be applied in the FPAA. It is, for one thing, crucial for achieving the aims of the FPAA for compliance therewith to be as clear and simple as possible. It should be borne in mind, however, that the statutory crimes of possession and distribution will require the State to prove intention to possess or distribute respectively and that the offences will be restrictively interpreted by the courts.

6.2. The obligation to report

The FPAA introduces an offence where a person who has knowledge of an offence involving child pornography or has reason to suspect that such offence has been or is being committed fails to report this as soon as possible to the South African Police Service (SAPS) and to provide all particulars upon request of the SAPS.

While it is obviously envisaged by the FPAA that ISPs will form a partnership with law enforcement agencies in fighting against child pornography this proposed "spirit of cooperation" does not, in the legal as opposed to moral sense, extend to a positive duty to actively monitor for offensive content or information indicative of offensive content. In other words the FPAA does not

[296] section 1(e) FPAA
[297] http://www.pmg.org.za/docs/2003/appendices/031118ispa.htm
[298] ECT Act s73
[299] ECT Act s72
[300] ECT Act s73(1)(a)-(d)
[301] ECT Act s73(2)(a)-(c)

contemplate anything other than knowledge or suspicion which is obtained during the course of the ordinary commercial activities of the ISP or through activities incidental thereto.

It may, in fact, well be the case that any active monitoring for child pornography may constitute an offence under RICA or a contravention of a provision of the expected data protection legislation.

The Canadian case of R v Weir[302], the facts of which are directly relevant to this discussion, illustrates the tension between the role of the ISP as custodian of personal information and its identified role in crime prevention and particularly child pornography.

Mr Weir, having exceeded his allowed disk space quota, requested his ISP to sort out the problem so that he would be able to access his mail. A technician employed by the ISP, following the standard procedure of opening files so as to allow attachments to be removed from the server, noticed that the names of some of the attachments were similar to names typically given to files containing child pornography. The technician duly reported this to his senior who in turn contacted the local police.

The reaction of the police was to demand that the ISP send the files to them while simultaneously reactivating Weir's account so that he would be able to download them and accordingly be in possession thereof. This was done, and on the basis of the ISP's sole initiative in alerting the police, the latter obtained a search warrant in execution of which Weir's hard drive was seized.

The trial court rejected Weir's argument to the effect that the ISP was performing a governmental function in assisting the police and that the search which it had undertaken was an unreasonable invasion of Weir's privacy and contrary to the constitutional right not to be subject to unlawful search and seizure.

Weir appealed this decision and based further argument that the ISP had been acting as an agent of the State on a criminal law doctrine known as "Broyles Test" [303], usually applied to informants set up by police to clandestinely record a confession. The crux of the doctrine is whether the exchange between the informer and the accused would have taken place, in the form and manner in which it did take place, but for the intervention of the State and its agents?[304]

The Court of Appeal, in applying Broyle to the facts of the matter, found that the ISP had indeed acted as an agent of the State when it had forwarded a copy of the e-mail and attachments to the police at their request. The search of Weir's home was accordingly unwarranted and the evidence obtained inadmissible.

The finding that an ISP acted as an agent of the state is highly significant when examining the changing roles of ISPs within society. The court in Weir explicitly acknowledges that ISPs are uniquely positioned to assist law enforcement agencies and therefore are no longer able to offer their clients any guarantees of confidentiality

Under the FPAA the discretion as to whether to report a suspected offence is removed from the hands of ISPs. By drawing an analogy from Weir's case an argument may be developed that one of the effects of the FPAA is to place ISPs in a position where they function as agents of the state and not as private body entities.

[302] 3d 59 Alta L.R., (Alta Q.B. 1998); R v Weir, 3d 95 Alta. L.R., 225 (Alta. C.A. 2001)
[303] see R v Broyles, 3 S.C.R. 595 (S.C.C. 1991)
[304] R v Broyles, 3 S.C.R. 595 (S.C.C. 1991) @ para 24

6.3. Registration & prevention of hosting and distribution of child pornography

Section 9 of the FPAA inserts a new section 27A into the principal Act, requiring every Internet service provider to:

(a) register with the Film & Publications Board in a manner prescribed by regulations yet to be promulgated; and
(b) take all reasonable steps to prevent the use of their services for the hosting or distribution of child pornography[305].

It appears that this registration requirement has been inserted both as means of control and as a means of allowing ISPs to limit their liability in respect of any actions which they may take pursuant to the Act. It is to be hoped that regulations setting out a limitation of liability regime will be published for comment in the near future.

ISPs are obliged, where they have knowledge that their services are in fact being used for the hosting or distribution of child pornography, to take all reasonable steps to prevent access to the child pornography by any person[306]. Where actual knowledge exists an ISP must report the presence of offending material together with details of the person(s) maintaining, hosting or distributing or in any manner contributing to such Internet address[307].

There are several difficulties with this requirement.

Firstly, the taking of all reasonable steps to prevent access to child pornography or remove offending material is a technologically complex task. It is extremely difficult, if not impossible, for an individual ISP to block access to content where the providers of the content are using floating domains and dynamic addressing with the effect that the site address is changed so frequently that ISPs cannot keep up. As is the case with aspects of RICA, this is a typical problem of virtual enforcement – the most serious providers and users of child pornography will remain largely unaffected by the FPAA due to advanced use of technology and encryption in the storing and transmission of child pornography. It would take the combined efforts of all tier1 ISPs in South Africa to even attempt to maintain a current listing.

Blocking access at ISP level has also been heavily criticised as being disproportionate in effect in that access is restricted to far more material than the targeted category of child pornography[308]. The European Parliament has voted overwhelmingly to oppose the use of blocking as a means of web content regulation[309]. EuroISPA, the largest ISP representative body in the world, has derided blocking as a "technically disastrous solution" which is "undoubtedly inefficient", aside from raising significant free speech and democratic concerns[310].

Secondly, there is the problem of defining child pornography and the probability that ISPs and others will err on the side of caution for both moral and legal reasons. This emphasises the need for an appropriate mechanism for protecting ISPs against civil claims based on a wrongful take-down of material or wrongful termination of services.

---

[305] FPAA section 9
[306] s27A(2)(a) of the principal Act
[307] s27A(2)(b) of the principal Act
[308] Akdeniz, Yaman "Governance of Pornography and Child Pornography on the Global Internet: A Multi-layered Approach" in Edwards, L & Waelde, C Eds., Law & the Internet: Regulating Cyberspace, Hart Publishing, 1997, pp223-241
[309] *Report on the Evaluation Report from the Commission to the Council and the European Parliament on the Application of the Council Recommendation of 24 September 1998 concerning the protection of minors and human dignity*, adopted by the European Parliament on 11 April 2002
[310] "European Parliament opposed Web Blocking" EuroISPA press release: 11 April 2002, available at www.euroispa.org

Finally, there is the problem of trying to enforce national laws and initiatives in the context of a problem that actively seeks to take advantage of different definitions, approaches and levels of enforcement across jurisdictions.

More realistic steps to be taken may include close co-operation between ISPs and hotlines set up to facilitate reporting of illegal content – in South Africa an opportunity exists for the ISP industry to take the initiative in setting up such a hotline and a single point of contact – and the implementation of content rating systems. ISPs should make every effort to provide consumers with clear and easy-to-use information on how to effectively control the content they see.

Section 27A(b)(3) provides, finally, that ISPs must furnish the particulars of users who gained or attempted to gain access to an Internet address that contains child pornography, "upon request by the South African Police Service".

Criminal sanctions are imposed for failure to comply with the above.

The ISPA submission[311] to the portfolio committee contains a plea on behalf of the industry that the increasing number of registration requirements on ISPs be streamlined and that a central database or repository be created under the control of ICASA or the Department of Communications. Within the context of ISPA's critique of the definition of ISPs in the FPAA this would mean that all ISPs which are licensed under the Telecommunications Act would be required to register with this central authority in order to obtain any exemptions or exceptions created by legislation.

It is submitted that this is the only approach which makes any sense and which will perhaps counteract the apparent lack of consistency in the way that ISPs are currently dealt with under different pieces of legislation.

6.4. Conclusion

It should be beyond doubt that the ISP industry in South Africa will seek to eradicate child pornography on the Internet and that it will work closely with the relevant law enforcement authorities of its own initiative. Most major SA ISPs already have explicit terms prohibiting the use of their networks for child pornography and have mechanisms in place through which its presence can be reported, even though these are seldom used.

It is submitted that the FPAA insofar as it purports to legislatively harness ISPs in the battle against child pornography evidences a disturbing tendency on the part of government in that it has not taken proper cognizance of the input and realities of the ISP industry. It remains to be seen to what extent ISPs and other access providers for the public good are realistically protected from prosecution where they have no physical or technological control over certain activities, and where they have taken steps to ensure that such activities are curtailed and eradicated[312].

When considering steps taken to comply with the obligations introduced by the FPAA, it would be advisable for ISPs to have a clear agreement with their staff and third parties with access to their systems to create binding guidelines with regard to the discovery of evidence of child pornography offences. These guidelines should canvass, *inter alia*,

- What grounds constitute "reason to believe" that that an offence has been or is being committed?
- Preservation of evidence
- Internal reporting procedures
- External reporting procedures; and

[311] found at http://www.pmg.org.za/docs/2003/appendices/031118ispa.htm (last visited 6 Sept 04)
[312] see http://www.pmg.org.za/docs/2003/appendices/031118ispa.htm (last visited 6 Sept 04)

- Restrictions imposed by RICA and forthcoming privacy legislation.

ISPs, both at industry and individual level, should have in place clear procedures as to the manner in which they will (a) take reasonable steps to ensure that their networks are not used for hosting or distributing child pornography and (b) take measures to remove or disable access to child pornography once they have been altered to its presence. The setting up of a single point of contact and dedicated hotlines would do much to evidence the seriousness with which ISPs view the threat of child pornography.

7. CONCLUSION

It is clear that the South African authorities, in line with trends in many other jurisdictions, have identified Internet service providers as being crucial to any attempt to impose regulation on the Internet and the people who use it for nefarious purposes. It should be equally clear that this will place ISPs in a position where they walk a tightrope between the expectations of their customers and their obligations to act as enforcement agents for the State – the "server-level" police.

The shift in the perceptions of ISPs on the part of consumers will require ISPs to take proactive steps. It is submitted that ISPs would be best served by doing their utmost to protect the privacy of the personal information of their customers and to deviate from this position only under proper, lawful authority. Any request or direction should be carefully examined by a qualified person to ensure that there has been a rigorous compliance with procedure by law enforcement agencies, although this should be achieved in a manner which does not alienate lawful applicants. Failure to comply with procedure by ISPs will expose them to both potential criminal sanctions under the Act as also claims for damages based on infringement of privacy. Prospective and existing customers should be made clearly aware of the legal obligations binding ISPs in respect of customer personal information and reassured that the ISP will attempt (without incurring liability) to ensure that information is only released where warranted.

Legislation such as RICA and the Film & Publications Act essentially involves a transfer of authority from public to private bodies, potentially placing ISPs in the position of judge and jury, a role which they should resist insofar as is possible. The point needs to be made that, at the end of the day, it is the collective responsibility of the State, ISP industry and society in general to ensure that the Internet is "cleaned up".

The industry should not shy away from making constitutional challenges to certain provisions of legislation such as RICA where this in both their own and their customers' interests.

As regards the problem of definition, ISPs provide an array of services and only some of the activities which they undertake justify their exclusion from the application of the law. This suggests that a definition of an ISP for legal purposes should focus on the exact nature of the activity which an organisation is undertaking rather than the nature or status of the organisation itself. Clarity as to the scope of application of the legislation considered in this paper is vital.

In conclusion this paper and the implications canvassed by it should serve as a clarion call to the industry to develop a far stronger voice in fighting for both the rights of ISPs to carry on their trade without undue interference and the customers' rights of their customers to privacy and freedom of expression. The industry is in flux and there are dark days ahead.

8. BIBLIOGRAPHY

Akdeniz, Yaman "Governance of Pornography and Child Pornography on the Global Internet: A Multi-layered Approach" in Edwards, L & Waelde, C Eds., Law & the Internet: Regulating Cyberspace, Hart Publishing, 1997, pp223-241

Chalet, A & Testro, L Are you an ISP? - Ambiguity in the Internet Censorship Legislation available at http://www.isoc-au.org.au/Regulation/PFoxBSA.html (last visited 3 September 2004)

Cyberlaw: The law of the Internet in South Africa, ed Buys, R Van Schaik Publishers 2000

Cyberlaw: The Law of the Internet in South Africa II, ed Buys, R Van Schaik Publishers 2004

Kerr, I & Gilbert D "The changing role of ISPs in the investigation of cybercrime" in Information Ethics in an Electronic Age: Current issues in Africa and the world, ed. Thomas Mendina & Johannes Britz (Jefferson, North Carolina: McFarland Press, 2004 (available from http://www.jisclegal.ac.uk/ispliability/ispliability.htm last visited 12 Sept 2004)

Marcovitch, S "Spam: Are there any technical solutions from ISPs?" presentation to OECD Workshop on Spam on behalf of EuroISPA, 2 February 2004, available at www.euroispa.org (last visited 22 Sept 2004)

Nash, Richard "A EuroISPA Perspective on Today's Policy, Business and Governance Issues", 17 October 2003, available at www.euroispa.org (last visited 22 Sept 2004)

Rotert, M "ISPs' Approach to Tackle Child Pornography on the Internet", EuroISPA presentation, 16 January 2004, available at www.euroispa.org (last visited 22 Sept 2004)

"European Parliament opposed Web Blocking" EuroISPA press release: 11 April 2002, available at www.euroispa.org

EUROISPA Response to Consultation Document on Traffic Data Retention, 15 September 2004 (available from www.euroispa.org, last visited 22 September 2004)

EUROISPA & USISPA position on the impact of data retention laws on the fight against cybercrime, 30 September 2002 (available from www.euroispa.org, last visited 22 September 2004)

SALC Discussion Paper 78, Project 105, Review of Security Legislation: The Interception and Monitoring Act 27 of 1992