6 December 2011

Ms Engela Steyn
State Law Adviser
Chief Directorate: Legislative Development
Department of Justice and Constitutional Development
East Tower Momentum Building E9.35
Pretorius Street
Pretoria

By e-mail: ensteyn@justice.gov.za

Dear Madam

PREVENTION AND COMBATING OF TRAFFICKING IN PERSONS BILL

1 In late November 2011 MWEB Connect (Pty) Limited ("MWEB") became aware of the Prevention and Combating of Trafficking in Persons Bill which, we understand, was tabled in the National Assembly on 16 March 2010.[1] We thank you for the opportunity to make urgent submissions on the Bill.

2 MWEB is an internet service provider ("ISP") and provides internet services and ancillary services such as Internet access, hosting, domain registration, and e-mail. MWEB is the holder of an electronic communications service licence ("ECS licence") and an electronic communications network service licence ("ECNS licence") issued to it by its regulator, the Independent Communications Authority of South Africa ("ICASA").

3 MWEB supports, in principle, initiatives to protect persons who are vulnerable to becoming victims of trafficking, and the enactment of appropriate legislation to deal with the problem of trafficking in persons.

4 However, MWEB is extremely concerned about the Bill's provisions as regards internet service providers as set out in s8(2) to (4) of the Bill. s8 is set out, for ease of reference, in **Annexure A**

---

[1] B7-2010. MWEB is working off the latest working draft of the Bill of the Parliamentary Portfolio Committee on Justice & Constitutional Affairs, dated 2 November 2011

5 We strongly oppose s8(2)(a), s8(3) and s8(4) of the Bill, for the reasons set out below. We also have serious concerns about s8(2)(b) of the Bill, which we deal with below.

Overview of MWEB's concerns

6 The Bill imposes inappropriate and disproportionate obligation on ISPs, with which it is virtually impossible for ISPs to comply. This is exacerbated by the unduly harsh consequences for non-compliance proposed by the Bill. We describe some of the practical realities faced by ISPs and explain the practical implications of s8 of the Bill, and the reasons why it is unreasonable, impractical, ineffective and excessively onerous, as well as some of the undesirable consequences likely to flow from s8(2) to (4) of the Bill.

7 The Bill departs significantly from the existing provisions of the Electronic Communications and Transactions Act, 2002 ("the ECT Act") and the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 ("RICA"), which contain lawful, reasonable and appropriate mechanisms, in line with international best practice, to deal with the role of service providers such as ISPs. The Bill also severely lacks the procedural safeguards, checks and balances of the ECT Act and RICA.

8 MWEB believes that s8(2)(a), s8(3) and s8(4) of the Bill unjustifiably infringe the Constitutional rights to freedom of expression, privacy, just administrative action and access to courts, and impinge on ISPs' freedom to conduct their business.

9 Furthermore, s8(2) to (4) of the Bill do not accord with international best practice.

10 The ECT Act and RICA already contains adequate mechanisms to achieve the objectives of s8(2) to (4) of the Bill. In addition, the common law regarding liability as an accomplice and the Bill's provisions regarding accomplices render s8(2)(a), s8(3) and s8(4) of the Bill unnecessary. s8 of the Bill is also not necessary in order to give effect to the Republic's international obligations.

11 MWEB supports s8(2)(b)(i) and (ii) of the Bill subject to our proposed amendment in paragraphs 100 to 103 below.

Bill imposes inappropriate and disproportionate obligation on ISPs

12 s8(2) to (4) of the bill would effectively require ISPs to monitor all of the communications of all of its customers, and to block certain communications, which may or may not, in fact, be unlawful.

13 It is virtually impossible for an ISP to suspect or know whether information facilitates or promotes trafficking in persons without actively monitoring all communications routed/facilitated by it.

14 s8(2)(a) of the Bill, which requires an ISP to take all reasonable steps to prevent the use of its service for the hosting of information which facilitates or promotes trafficking in persons, failing which it will be guilty of an offence[2] and liable to have its licence revoked,[3] is particularly unfeasible, disproportionate and harsh.

15 The practical implication of s8(2) of the Bill is that it could require ISPs, to, amongst other things –

15.1 actively intercept and monitor all communications (including all attachments thereto), regardless of their nature, content, size, sender or recipient, and without any cause for suspicion;

15.2 assess all of the electronic communications of all its customers and identify the files which could potentially facilitate or promote trafficking in persons;

15.3 determine which of those files contain data/information which is potentially prohibited by the Bill (i.e. which the ISP considers to be unlawful);

15.4 make a call on whether it is indeed unlawful;

15.5 take all reasonable steps to prevent access to (i.e. block) an internet address on its server that contains such information; and

15.6 install a complicated, costly, permanent computer system and appoint employees, consultants and advisors, at its own expense, for this purpose.

16 The Bill's proposals must be considered against the background of the practical realities faced by ISPs. As but a few examples -

16.1 there are 1.9 Billion internet users worldwide;

16.2 there were 255 Million websites at the end of December 2010;

16.3 Facebook is the most used website. 175 Million users log on to Facebook every 24 hours;

16.4 25 Billion Tweets were sent in 2010;

16.5 107 Trillion emails were sent in 2010;

16.6 approximately 294 Billion email messages are sent per day; and

---

2 s8(3) of the Bill

3 s8(4) of the Bill

16.7 there are 1,88 Billion users of email worldwide.[4]

17 MWEB alone has more than 300 000 subscribers. On average, MWEB receives 12.8 Million incoming mail connections per day (including spam) (approximately 400 Million incoming mail connections per month). This figure sometimes increases to over 16 Million incoming e-mails per day.

18 By way of further illustration, a Google search for the phrase "human trafficking" yielded 13.2 million hits. The terms human trafficking (not linked as a phrase) yielded 23 million hits. A quick skim of the first 100 hits reflected websites trying to create an awareness of and curb human trafficking. Many of these websites contained the words "sex" and "prostitution".

19 It is thus virtually impossible for an ISP such as MWEB to know or suspect which websites or e-mails are used by third parties to facilitate or promote trafficking in persons, unless specific unlawful activity is actively brought to its attention. Whilst word filters may seem like an easy option, they are in fact ineffective because, amongst other things –

19.1 the list of possible words which a human trafficking website could use for its unlawful activities are limitless and cannot be predicted by a service provider;

19.2 filters would need to cater for an endless permutation of languages, slang, local dialects, and synonyms;

19.3 domain names/website addresses (URLs) are not necessarily a true reflection of a website's purpose or content;

19.4 offenders evade filtering techniques by using constantly changing terminology and ploys, and regularly changing file names, file sites, website addresses and website hosts;

19.5 many words which could be used to advertise human and sex trafficking could equally be used for legitimate activities (such as the use of the word "breast" in a breast cancer awareness site or "sex" in a website on sex education, sexually transmitted diseases or HIV/AIDS awareness campaigns; and

19.6 filters are unable to distinguish between lawful and unlawful content.

---

[4] Statistics gathered & Compiled by Gillian Meier, Digital Media Strategist & Trainer, from various sources such as the Mobile Marketing Association, World Wide Worx and a number of South African speakers and presenters from various Mobile & eCommerce Marketing events held in June & July 2011. These statistics are intended by the compiler purely for reference purposes, and the compiler recommend that you verify them before using them in any research material. They are referred to here as being broadly indicative of the ISP landscape in South Africa and the rest of the world (http://www.bluemagnet.co.za/content/view/87/168/, last visited 29 November 2011)

20 The blocking of an internet address would unavoidably block both lawful and infringing content. ISPs do not have the skills, resources or ability to properly establish the lawfulness of third party content. Nor is it reasonable to expect ISPs to do so.

21 For example, several years ago in Pennsylvania, due to the commercial and technical practicalities of statutory blocking requirements, ISPs disabled access to approximately 1.19 million innocent websites. The legislation was subsequently found to be unconstitutional.[5]

22 Amongst others, s8 of the Bill begs the following questions:

22.1 How could an ISP know which communications facilitate or promote trafficking in persons? ISPs have no control over content/communications because these sites are based on third party content. As we have indicated above, ISPs transmit countless messages over their information systems and are not in a position to identify unlawful content.

22.2 What would constitute "reasonable steps to prevent the use of its service for the hosting of information which facilitates or promotes trafficking in persons"? MWEB submits that any requirement to actively intercept and/or monitor communications or to carry out any of the other activities mentioned in paragraph 15 above is not reasonable.

22.3 On what basis would an ISP determine whether or not communications are unlawful? For the reasons we indicated in paragraphs 20 and 21 above, it is inappropriate and unreasonable to task ISPs with law enforcement and judicial functions.

22.4 What happens if an ISP prevents the hosting of information which is not unlawful, or takes steps to prevent access to an internet address used for lawful purposes?

22.5 Will the Department of Justice (or any other party) indemnify ISPs for liability incurred as a result of the ISP's conduct in terms of s8 of the Bill? (e.g. due to the *bona fide* prevention by an ISP of the hosting of information or access to an internet address where the activities concerned are subsequently found to be lawful; for infringement of a person's right to privacy; for damage to a person's reputation or loss of earnings, etc.)

23 s8(2)(a), s8(3) and s8(4) of the Bill are therefore unreasonable and inappropriate, and impose a disproportionate and harsh obligation on ISPs.

---

5 *Center for Democracy & Technology v Pappert* 337 F Supp 2d 606 (ED Pa 2004)

24 Furthermore, the ECT Act, RICA, the Criminal Procedure Act, 1977, and the common law already contain adequate and appropriate provisions for ISPs to assist law enforcement authorities in an appropriate manner, which provides for due process and is more narrowly tailored to avoid infringing on Constitutional rights. We elaborate on this below.

Electronic Communications and Transactions Act, 2002

25 s8(2) to (4) of the Bill depart significantly from the current statutory position governing the liability of ISPs.

26 Chapter 11 of the ECT Act deals with the liability of service providers[6] such as ISPs.

27 It creates a reasonable and appropriate statutory framework which adopts several measures to balance service providers' rights and obligations in the public interest with the practical realities faced by such service providers.

28 Three of the core principles of Chapter 11 of the ECT Act which are most relevant for present purposes are set out below. Chapter 11 of the ECT Act is set out in full in **Annexure B**.

No general obligation to monitor

29 The ECT Act expressly provides that there is no general obligation on a service provider to monitor the data which it transmits or stores, or to actively seek facts or circumstances indicating an unlawful activity.[7]

30 The ECT Act thus recognises that, given the extent of the data which a service provider transmits or stores, the service provider's passive role in that process, Constitutional rights and public policy considerations, a service provider cannot, and should not, be expected to monitor the data which it transmits and stores.

31 This accords with the right to privacy in s14 of the Constitution, as well as the provisions of RICA (which we deal with below).

32 The Minister of Communications may, subject to s14 of the Constitution[8], prescribe procedures for service providers to –

---

6 "Service Provider" is defined as meaning "any person providing information system services". (s70 of the Bill) "Information system services" is defined in s1 of the ECT Act as including "the provision of connections, the operation of facilities for information systems, the provision of access to information systems, the transmission or routing of data messages between or among points specified by a user and the processing and storage of data, at the individual request of the recipient of the service". "Information system" is defined in s1 of the ECT Act as meaning "a system for generating, sending, receiving, storing, displaying or otherwise processing data messages, and includes the internet."

7 s78(1) of the ECT Act

8 s14 of the Constitution gives every person the right to privacy, including the right not to have the privacy of their communications infringed

32.1 inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service; and

32.2 to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service.[9]

Mere conduit

33 A service provider will not be liable for providing access to, or for operating facilities for, information systems, or transmitting, routing or storing data messages via an information system under its control, if the service provider –

33.1 does not initiate the transmission;

33.2 does not select the addressee;

33.3 performs the functions in an automatic, technical manner without selection of the data; and

33.4 does not modify the data contained in the transmission.[10] [11]

34 In other words, where the service provider merely distributes data via its information system, but does not control it, the service provider is a "mere conduit". The ECT Act recognises that it is not feasible, reasonable or appropriate to visit liability upon a mere conduit, given its passive role in this process.

35 Notwithstanding the "mere conduit" provisions of the ECT Act, a competent court may order a service provider to terminate or prevent unlawful activity in terms of any other law.[12]

Take down notifications

36 Any person may, in writing, lodge a notification of unlawful activity with a service provider in accordance with s77 of the ECT Act.

37 A service provider must remove or disable access to data upon the receipt of a take down notification.[13]

---

9 s78(2) of the ECT Act

10 s73(1) of the ECT Act

11 The acts of transmission, routing and of provision of access include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place -

- for the sole purpose of carrying out the transmission in the information system;
- in a manner that makes it ordinarily inaccessible to anyone other than anticipated recipients; and
- for a period no longer than is reasonably necessary for the transmission (s73(2) of the ECT Act)

12 s73(3) of the ECT Act

13 s77 of the ECT Act read with s74(1)(e) and s75(1)(c) of the ECT Act

38 By virtue of s77(3) of the ECT Act, a service provider will not be liable for wrongful take-down in response to a notification.

39 The Minister of Communications has prescribed Guidelines for the Recognition of Industry Representative Bodies of Information Systems Service Providers[14] which reinforces these principles, and, amongst other things, contains take down procedures.

40 Thus, the ECT Act provides for unlawful activity to be notified to the relevant service provider, who must then remove or block that data subject to the notice and take down procedures.

41 In this way, the ECT Act already provides an appropriate mechanism for a service provider to remove and block access to unlawful data, subject to –

41.1 unlawful activity having been brought to the service provider's attention, in the appropriate manner, and subject to due process; and

41.2 the assurance that the service provider will not be exposed to liability for wrongful take-down in response to a notification.

42 This alleviates the undesirable situation where a service provider is unreasonably expected to "blanket" monitor all communications transmitted or routed by it, identify potentially unlawful activity, make a decision on whether or not it is unlawful, and risk blocking content which may subsequently be found to be lawful.

Chapter 11 of ECT Act accords with international best practice

43 The ECT Act is in line with international best practice. In particular, Chapter 11 of the ECT Act accords with the European Union E-Commerce Directive,[15] which contains substantially similar provisions on the liability of service providers.[16] The Recitals to the E-Commerce Directive contextualise those provisions:

> "This Directive strikes a balance between the different interests at stake and establishes principles upon which industry agreements and standards can be based.
>
> The exemptions from liability ... cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this

[14] Gazette No. 29474, Notice No. 1283, 14 December 2006

[15] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on Electronic Commerce) ("the E-Commerce Directive")

[16] s73 to 78 of the ECT Act mirror articles 12 to 15 of the E-Commerce Directive.

activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.

A service provider can benefit from the exemptions for "mere conduit" and for "caching" when he is in no way involved with the information transmitted; this requires among other things that he does not modify the information that he transmits; ....

A service provider who deliberately collaborates with one of the recipients of his service in order to undertake illegal acts goes beyond the activities of "mere conduit" or "caching" and as a result cannot benefit from the liability exemptions established for these activities.

...

In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level ...."[17]

Concluding comments re ECT Act

44 The ECT Act already contains adequate mechanisms for service providers such as ISPs to assist law enforcement authorities tackle unlawful activities such as human trafficking, subject to due process. More specifically, as we indicated above –

44.1 the Minister of Communications may prescribe procedures for service providers to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service, and to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service;[18]

44.2 a service provider must remove or disable access to data in respect of unlawful activity upon the receipt of a take down notification;[19] and

44.3 a competent court may order a service provider to terminate or prevent unlawful activity in terms of any other law.[20]

---

17 Recitals to the E-Commerce Directive

18 s78(2) of the ECT Act

19 s77 of the ECT Act read with s74(1)(e) and s75(1)(c) of the ECT Act

20 s73(3), s74(2) and s75(3) of the ECT Act

45 Furthermore, an ISP's liability would be limited in terms of Chapter 11 of the ECT Act only where the ISP acted as a "mere conduit", etc. Thus, to the extent that an ISP knowingly committed, or facilitated the commission of, an offence in terms of the Bill, the ISP would not escape liability/prosecution.

46 Chapter 11 of the ECT Act is in line with international best practice. It strikes a balance between requiring service providers to assist law enforcement initiatives, subject to due process, without requiring service providers to monitor communications or exposing them to liability for wrongful take down.

RICA

47 To the extent that the Bill requires (by implication) the interception and monitoring of communications, it conflicts with RICA.

48 As the Department of Justice is no doubt aware, RICA prohibits the interception of communications unless it is authorised by or pursuant to RICA. s2 of RICA provides:

> "Subject to this Act, no person may intentionally intercept or attempt to intercept, or authorise or procure any other person to intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission."

49 <u>RICA already provides for interception by a service provider such as MWEB, subject to the numerous checks and balances in that Act.</u>

50 The interception contemplated in RICA (whilst already onerous and expensive for service providers such as MWEB) does not go as far as the Bill. Amongst other things:

50.1 RICA does not require service providers to conduct general "blanket" monitoring in respect of all of the communications of all of its customers.

50.2 RICA does not require service providers to fulfil the role of police, judge and jury.

50.3 A service provider's obligation is limited in respect of a specific identified person, in respect of specific content, following the issue of an interception order which complies with the procedural safeguards in RICA and the Criminal Procedure Act.

50.4 The service provider does not carry out any monitoring itself – it merely forwards the relevant content to the law enforcement authorities concerned.

51 One of the ways in which RICA is much more narrowly tailored than the Bill, is the existence of detailed provisions in RICA to ensure that the obligation on service providers is more reasonable and proportionate, and that the constitutional rights of affected persons are not unjustifiably infringed.

52 RICA provides for interception and monitoring to take place only in limited circumstances and provided that stringent procedural safeguards have been met.[21] By way of example, s16 of RICA contains detailed provisions, including extensive procedural safeguards, for an application for, and the issuing of, an interception direction. Amongst other things –

52.1 an application for an interception direction must–

52.1.1 be made to a designated judge;[22]

52.1.2 be in writing;[23]

52.1.3 indicate the identity of the applicant and of the law enforcement officer who will execute the interception direction (if known and appropriate), the person or customer (if known) whose communication is required to be intercepted, and the postal or telecommunication service provider to whom the direction must be addressed (if applicable);[24]

52.1.4 specify the grounds on which the interception order may be made;[25]

52.1.5 contain full particulars of all the facts and circumstances alleged by the applicant in support of the application;[26]

52.1.6 describe the nature and location of the facilities from which, or the place at which, the communication is to be intercepted (if known), the type of communication which is required to be intercepted, and the basis for believing that evidence relating to the ground on which the application is made will be obtained through the interception;[27]

52.1.7 contain information about other investigative procedures to procure the required evidence[28] and whether any previous application has been made for the issuing of an interception direction in respect of the same person or customer, facility or place;[29] and

---

21 Chapter 3 of RICA deals with applications for, and the issuing of, directions and entry warrants
22 s16(1) of RICA
23 s16(2) of RICA
24 s16(2)(a) of RICA
25 s16(2)(b) of RICA
26 s16(2)(c) of RICA
27 s16(2)(d) of RICA
28 s16(2)(e) of RICA
29 s16(2)(g) of RICA

52.1.8 indicate the period for which the interception direction is required to be issued.[30]

53 An interception direction may be issued only if the designated judge concerned is satisfied, based on the facts alleged in the application concerned, that there are reasonable grounds to believe that certain requirements have been met (e.g. that a serious offence has been or is being or will probably be committed), and that there are reasonable grounds to believe that the interception of particular communications will be obtained by means of such an interception direction, etc.[31]

54 An interception direction must be in writing, must contain certain information, may specify conditions or restrictions relating to the interception of communications authorised therein, and must be issued for a specified period which may not exceed three months.[32]

55 This is not an exhaustive description of RICA's requirements. Rather, we have, for illustrative purposes, described some of the requirements for an interception order in order to demonstrate the detailed checks and balances which must be met in order for any interception to be carried out lawfully in terms of RICA.

56 s8 of the Bill contains no equivalent safeguards. In the circumstances, s8(2)(a), s8(3) and s8(4) of the Bill are unlikely to withstand Constitutional scrutiny. We elaborate on our Constitutional concerns below.

Constitutional concerns

Freedom of expression

57 As we indicated in paragraphs 20 and 21 above, s8(2) to (4) of the Bill effectively require an ISP to monitor communications transmitted on its information system (lawful and unlawful alike) and to block access to communications which that ISP considers unlawful, with the likelihood of unavoidably blocking both lawful and infringing content

58 s8(2) to (4) of the Bill accordingly infringe on the right to freedom of expression entrenched in s16 of the Constitution.

59 Where the state extends the scope of regulation beyond expression envisaged in section 16(2), it encroaches on the terrain of protected expression and can do so only if such regulation meets the justification criteria in section 36(1) of the Constitution."[33]

---

30 s16(s)(f) of RICA

31 s16(5) of RICA

32 s16(6) of RICA

33 *Islamic Unity Convention v Independent Broadcasting Authority and Others*, 2002 (4) SA 294 (CC)

60 The Constitutional Court has emphasised "the two-sided nature of the right, not only to impart information but also to receive it". It concluded:

> "Could less restrictive means have been used to achieve the purpose of the regulation in this instance? Without prejudging the constitutionality of the IBA proposals in the position paper, it is clear that they are much less invasive of the right to freedom of expression and there is nothing to indicate that they would be any less effective in achieving the purpose of regulation.
>
> There is no doubt that the inroads on the right to freedom of expression made by the prohibition on which the complaint is based are far too extensive... It has also not been shown that the very real need to protect dignity, equality and the development of national unity could not be adequately served by the enactment of a provision which is appropriately tailored and more narrowly focused. I find therefore that the relevant portion of clause 2(a) impermissibly limits the right to freedom of expression and is accordingly unconstitutional." [34]

61 MWEB submits that s8(2)(a), read with s8(3) and s8(4) of the Bill unjustifiably infringe the right to freedom of expression in s16 of the Constitution.

Right to privacy

62 In order to comply with s8(2)(a) of the Bill, ISPs would effectively be required to monitor and assess all communications (whether lawful or not), on an ongoing basis, without cause for suspicion of unlawful activity, without an interception order.

63 Unlike s78(2) of the ECT Act, s8 of the Bill is not subject to s14 of the Constitution. Nor does the Bill contain safeguards such as those in RICA (which we dealt with at length above) to protect peoples' right to privacy, and specifically the right not to have the privacy of their communications infringed.

64 MWEB accordingly submits that s8(2) to (4) of the Bill unjustifiably infringe the right to privacy of third parties, including the right not to have the privacy of their communications infringed, in terms of s14 of the Constitution.

65 We refer in this regard to the European Court of Justice's conclusion in the Scarlet decision (which we referred to in paragraphs 84 to 86 below) that the contested filtering system violated the right to privacy. For similar reasons, MWEB submits that s8(2) to (4) of the bill will not withstand scrutiny against s14 of the Constitution.

Just administrative action and access to courts

66 MWEB submits that s8(2)(a) of the Bill violates the right of individuals to due process (just administrative action) and access to courts, in that it requires ISPs

---

[34] *Islamic Unity Convention v Independent Broadcasting Authority and Others*, 2002 (4) SA 294 (CC)

to exercise their discretion and make a unilateral decision on the lawfulness of communications, without affording the individuals concerned an opportunity to be heard, effectively rendering the ISP police, judge and jury.

67 The Bill requires online content be removed without a court order and without any requirement for the third party concerned to receive any notice prior to its removal.

68 s8 of the Bill provides for the unfair removal of lawful content without due process, right of appeal, right of review or transparency or other procedural safeguards.

69 This is, once again, in stark contrast to the extensive procedural safeguards in RICA.

Concluding comments re Constitutional concerns

70 The internet is an unprecedented platform for innovation, speech, collaboration, civic engagement, and economic growth. Whilst it is regrettably used as a tool by criminals for unlawful activities such as the trafficking in persons, the Bill should not stifle the benefits of the Internet or infringe Constitutional rights.

71 s8(2) to (4) of the Bill imposes onerous and unfeasible obligations on ISPs, and incredibly harsh consequences for the failure to comply.

72 In any event, MWEB believes that s8(2) to (4) of the Bill is an ineffective tool to address human trafficking concerns, and that s8(2) to (4) of the Bill will not achieve its objective of combating the demand for the services of victims of trafficking. s8(2) to (4) of the Bill is inappropriate and is unlikely to withstand Constitutional scrutiny.

s8(2) to (4) of the Bill do not accord with international best practice

United States of America

73 Several court decisions in the United States of America ("the USA") have, for similar reasons to those dealt with above, struck down legal provisions which sought to prohibit the use of the internet for sending indecent material.

74 The Communications Decency Act,1996 ("CDA") sought to protect minors against pornography, including by criminalising the transmission of materials that were "obscene" to minors.

75 In 1996 the US Supreme Court struck down as unconstitutional provisions of the CDA which would have made it an offence to communicate anything "indecent" on the Internet, and which criminalised the knowing transmission of indecent messages to minors on the basis that they were overbroad, had the

effect of blocking both lawful and unlawful content, and violated freedom of expression.[35]

76 In this regard, the US Supreme Court held:

> "We are persuaded that the CDA lacks the precision that the First Amendment requires when a statute regulates the content of speech. In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another. That burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve."[36]

77 The Court concluded:

> "We agree with the District Court's conclusion that the CDA places an unacceptably heavy burden on protected speech, and that the defenses do not constitute the sort of 'narrow tailoring' that will save an otherwise patently invalid unconstitutional provision. In *Sable*, 492 U. S., at 127, we remarked that the speech restriction at issue there amounted to "'burn[ing] the house to roast the pig.' " The CDA, casting a far darker shadow over free speech, threatens to torch a large segment of the Internet community."[37]

78 In response to that decision, Congress enacted the Child Online Protection Act ("COPA"), which provided for civil and criminal penalties for any person who "knowingly posted 'material that is harmful to minors' on the Web 'for commercial purposes.'"[38]

79 The United States Court of Appeals[39] considered COPA's provisions and held as follows:

> "COPA endangers a wide range of communications, exhibits, and speakers whose messages do not comport with the type of harmful materials legitimately targeted under COPA, i.e., material that is obscene as to minors. Accordingly, while COPA penalizes publishers for making available improper material for minors, at the same time it impermissibly burdens a wide range of speech and exhibits otherwise protected for adults. Thus, in our opinion, the Act, which proscribes publication of material harmful to minors, is not

---

35 *RENO v ACLU*, 521 U.S. 844

36 *RENO v ACLU*, 521 U.S. 844, pg 874

37 *RENO v ACLU*, 521 U.S. 844, pg 881 to 882

38 COPA contained "'affirmative defenses' available to publishers, which require the technological screening of users for the purpose of age verification"

39 Third Circuit

narrowly tailored to serve the Government's stated purpose in protecting minors from such material."[40]

80 On appeal, the Supreme Court upheld the Court of Appeals' decision. It held:

> "Content-based prohibitions, enforced by severe criminal penalties, have the constant potential to be a repressive force in the lives and thoughts of a free people. To guard against that threat the Constitution demands that content-based restrictions on speech be presumed invalid, R.A.V. v. St. Paul, 505 U.S. 377, 382, 112 S.Ct. 2538, 120 L.Ed.2d 305 (1992), and that the Government bear the burden of showing their constitutionality. United States v. Playboy Entertainment Group, Inc., 529 U.S. 803, 817, 120 S.Ct. 1878, 146 L.Ed.2d 865 (2000). This is true even when Congress twice has attempted to find a constitutional means to restrict, and punish, the speech in question."[41]

81 The Supreme Court affirmed the decision that COPA violated the First Amendment because COPA was not the least restrictive means available for the Government to prevent minors from using the Internet to gain access to harmful materials. In particular, both Courts found that the use of filtering systems by parents should be promoted to restrict content which parents consider harmful to, or inappropriate for, their children. The Supreme Court stated:

> "By enacting programs to promote use of filtering software, Congress could give parents that ability [to monitor what their children see] without subjecting protected speech to severe penalties."[42]

82 User-controlled filters were held to be preferable because they "impose selective restrictions on speech at the receiving end, not universal restrictions at the source". The Court stated:

> "Promoting the use of filters [by parents] does not condemn as criminal any category of speech, and so the potential chilling effect is eliminated, or at least much diminished. Filters [by parents], moreover, may well be more effective than COPA.
>
> ...
>
> By enacting programs to promote use of filtering software, Congress could give parents that ability without subjecting protected speech to severe penalties."[43]

---

[40] *American Civil Liberties Union v. Ashcroft*, 322 F.3d 240 ("ACLU II"), pg 253

[41] *Ashcroft v American Civil Liberties Union*, 542 U.S. 656 (2004) ("*Ashcroft v ACLU*")

[42] *Ashcroft v ACLU*, pg 13

[43] *Ashcroft v ACLU*, pg 8 – 9, and 11 - 12

83 In 2008 the US Supreme Court of Appeal, once again, struck down provisions of COPA as unconstitutional, concluding, once again, that user-based blocking and filtering software is a more effective way of protecting minors from exposure to harmful material on the internet and are less restrictive on the rights to freedom of speech and expression than COPA because they impose selective restrictions on speech at the receiving end, rather than universal restrictions at the source.[44] In January 2009 the US Supreme Court refused to hear appeals of the lower court decision.

European Union

84 On 24 November 2011 the European Court of Justice handed down a judgment which concluded that European law precluded an injunction which required an ISP to install a blanket filtering system to address intellectual property rights infringements by third parties, because, inter alia, it infringed ISPs' customers' freedom of expression.[45] The European Court of Justice held as follows:

> "Preventive monitoring of this kind would thus require active observation of all electronic communications conducted on the network of the ISP concerned and, consequently, would encompass all information to be transmitted and all customers using that network."[46]

85 The injunction would have required the installation of a filtering system which would have involved –

> "monitoring all the electronic communications made through the network of the ISP concerned in the interests of those rightholders. Moreover, that monitoring has no limitation in time, is directed at all future infringements and is intended to protect not only existing works, but also future works that have not yet been created at the time when the system is introduced."[47]

86 The contested filtering system was accordingly prohibited by European law. The European Court of Justice stated:

> "Moreover, the effects of that injunction would not be limited to the ISP concerned, as the contested filtering system may also infringe the fundamental rights of that ISP's customers, namely their right to protection of their personal data and their freedom to receive or impart information, which are rights safeguarded by Articles 8 and 11 of the Charter respectively.
>
> It is common ground, first, that the injunction requiring installation of the contested filtering system would involve a systematic analysis of all content

---

44 *ACLU v Mukasey*, United States Court of Appeals for the Third Circuit, Case No No. 07-2539

45 The Scarlet Decision, para 54

46 *Scarlet Extended SA vs Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (and Others)*, Judgement of the European Court of Justice (Third Chamber), 24 November 2011, Case C-70/10 ("the Scarlet decision"), para 39

47 The Scarlet decision, para 47

and the collection and identification of users' IP addresses from which unlawful content on the network is sent. Those addresses are protected personal data because they allow those users to be precisely identified.

Secondly, that injunction could potentially undermine freedom of information since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications ...

Consequently, it must be held that, in adopting the injunction requiring the ISP to install the contested filtering system, the national court concerned would not be respecting the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the other." [48]

87 The Court also held that the contested filtering system violated ISPs' freedom to conduct business. It held as follows:

"Accordingly, in circumstances such as those in the main proceedings, national authorities and courts must, in particular, strike a fair balance between the protection of the intellectual property right enjoyed by copyright holders and that of the freedom to conduct a business enjoyed by operators such as ISPs pursuant to Article 16 of the Charter.

...

Accordingly, such an injunction would result in a serious infringement of the freedom of the ISP concerned to conduct its business since it would require that ISP to install a complicated, costly, permanent computer system at its own expense, which would also be contrary to the conditions laid down in Article 3(1) of Directive 2004/48, which requires that measures to ensure the respect of intellectual-property rights should not be unnecessarily complicated or costly.

In those circumstances, it must be held that the injunction to install the contested filtering system is to be regarded as not respecting the requirement that a fair balance be struck between, on the one hand, the protection of the intellectual-property right enjoyed by copyright holders, and, on the other hand, that of the freedom to conduct business enjoyed by operators such as ISPs.

Republic's obligations concerning the trafficking of persons in terms of international agreements

88 One of the Bill's primary purposes is to give effect to the Republic's obligations concerning the trafficking of persons in terms of international agreements, such

[48] The Scarlet Decision, paras 50 to 53

as the United Nations Protocol to Prevent, Suppress and Punish Trafficking in Persons ("the UN Protocol").[49]

89 As we indicated above, MWEB supports such initiatives to the extent that they are reasonable and appropriate.

90 However, s8(2)(a), 8(3) and 8(4) of the Bill go way beyond what is necessary to give effect to the UN Protocol. The UN Protocol does not contain any provisions which would require the Republic of South Africa to enact legislation regarding internet service providers as contemplated in s8 of the Bill. Nor does s8 of the Bill find support therein.

Adequate existing remedies in ECT Act, RICA, at common law and the Bill

ECT Act and RICA

91 As we have demonstrated above, the ECT Act and RICA already contain adequate and appropriate provisions to achieve the objectives of s8 of the Bill.

Common law liability as an accomplice

92 An ISP could also face prosecution at common law as an accomplice to the trafficking in persons to the extent that it knowingly furthers, assists or facilitates the commission of an offence.

93 A person can be punished if he unlawfully and intentionally furthers the crime committed by someone else by, giving the latter advice or assisting him. He is then an accomplice.[50]

94 In order for an ISP to do so "knowingly", intention must be present.[51] There are three forms of intention, namely "*dolus directus*"[52], "*dolus indirectus*"[53] and "*dolus eventualis*"[54], all qualifying equally as intention.

---

49 Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, Supplementing the United Nations Convention Against Transnational Organised Crimes

50 *S v Jackelson* 1920 AD 486, *S v William* 1980 (1) SA 60 (A)

51 *LAWSA*, Second Edition, Vol 17, pg 127, para 159

52 Where *dolus directus*, also called actual intention, is present, a person directs his or her will to bringing about the prohibited act or consequence and deliberately accomplishes what he or she actually intended and desired to accomplish

53 *Dolus indirectus* exists where a person foresees that a certain consequence will inevitably follow his or her achieving his or her aim (*dolus directus*) and the person nevertheless acts

54 This form of intention "exists where the accused does not 'mean' to bring about the unlawful circumstances or to cause the unlawful consequence which follows from his or her conduct, but foresees the possibility ... that the prohibited consequence might occur, in substantially the same manner as that in which it actually does occur, or the prohibited circumstance might exist and ... [the accused] accepts this possibility ... (i.e. is reckless as regards this possibility)." (*Principles of Criminal Law*, J Burchell, Third Edition, pgs 462 and 467) The requirements are therefore foresight, possibility, a correlation between the foreseeing and the actual manner of consequence occurring, and recklessness. It would be for the prosecution to prove each of these

95 Given the common law provisions in that regard, it is not necessary for South Africa to enact legislation to establish as a criminal offence the participation as an accomplice in an offence.

The Bill

96 Notwithstanding our comments in paragraphs 91 to 95 above, to the extent that the Department of Justice still believes that it is necessary to enact legislation to deal with accomplices, MWEB submits that s10 of the Bill is adequate.

97 Any person who (a) attempts to commit or performs any act aimed at participating in the commission of; (b) incites, instigates, commands, directs, aids, promotes, advises, recruits, encourages or procures any other person to commit; or (c) conspires with any other person to commit, an offence under Chapter 3 of the Bill will be guilty of an offence.[55]

98 This gives effect to Art 5(2)(b) of the UN Protocol, which requires party states to adopt legislative and other measures as may be necessary to establish as a criminal offence the participation as an accomplice in an offence.

99 One of the factors which the Bill proposes be considered in sentencing is the significance of the role of the convicted person in the trafficking process.[56] This is appropriate and necessary in order to deal with the varying roles of the parties involved.

Reporting to relevant authorities

s8(2)(b)(i) and (ii) of the Bill

100 Subject to our proposed amendment in paragraph 101 below, MWEB supports s8(2)(b)(i) and (ii) of the Bill, which provide that "an internet service provider operating in the Republic that has knowledge that any internet address on its server contains information referred to in subsection (1)(c) must -

(i) without delay report that internet address, as well as the particulars of the person maintaining or in any manner contributing to that internet address, to the South African Police Service;

(ii) take all reasonable steps to preserve any evidence for purposes of investigation and prosecution by the relevant authorities..."

101 The opening sentence to s8(2)(b) should be amended to refer to "actual" knowledge.

---

[55] s10 of the Bill

[56] s14(a) of the Bill

s8(2)(b)(iii) of the Bill

102 MWEB opposes s8(2)(b)(iii) of the Bill, which requires an ISP that has knowledge that any internet address on its server contains information referred to in subsection (1)(c) of the Bill to, "without delay take all reasonable steps to prevent access to that internet address by any person".

103 Given the risk of liability faced by an ISP for wrongful take down, MWEB proposes that s8(2)(b)(iii) of the Bill be amended to –

103.1 require an ISP to block access to content pursuant to a take down notice in terms of the ECT Act; and

103.2 indemnify ISPs against liability for wrongful take down, to the extent that the ISP blocked access to content pursuant to a take down notice.

Conclusion

104 MWEB submits that s8(2)(a), s8(3) and s8(4) of the Bill are an inappropriate and ineffective tool to address concerns about the trafficking of persons. It does not accord with the ECT Act, RICA or international best practice.

105 s8(2)(a), s8(3) and s8(4) of the Bill unjustifiably infringe the rights to freedom of expression, privacy, just administrative action and access to courts, and impinge on ISPs' freedom to conduct their business.

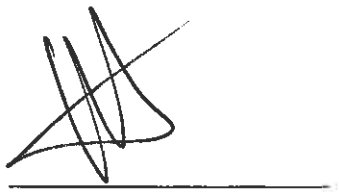
106 Those provisions are not necessary in order to comply with the Republic's international obligations. Nor are they necessary at all, because the ECT Act, RICA, the common law and the Bill already contain adequate effective and appropriate tools to achieve such objectives.

107 MWEB further submits that the proposed penalties are excessively harsh and inappropriate in the light of the passive role of ISPs, who merely distribute third party content as a mere conduit, and interfere with ICASA's regulatory and licensing activities.

108 MWEB therefore proposes that s8(2), 8(3) and (4) of the Bill be deleted, save for s8(2)(b), which we propose be amended as suggested in paragraphs 100 to 103 above.

109 MWEB would welcome an opportunity to meet with you to discuss this matter further and to provide you with any necessary clarity.

Yours sincerely



Wilmari Hannie
Head of Legal
Tel: 021 596 8533
Fax: 021 596 8715

MWEB Connect (Pty) Ltd

ANNEXURE A: S8 OF THE BILL

"Conduct facilitating trafficking in persons

(1) Any person who —

(a) intentionally leases or subleases any room, house, building or establishment for facilitating or promoting trafficking in persons or allows it to be used or ought reasonably to have known or suspected that it will be used to facilitate or promote trafficking in persons; or

(b) subsequent to the lease or sublease of any room, house, building or establishment, becomes aware or ought reasonably to have known or suspected that it is being used to facilitate or promote trafficking in persons and fails to report that knowledge to a police official;

(c) advertises, publishes, prints, broadcasts, distributes or causes the advertisement, publication, printing, broadcast or distribution of information that facilitates or promotes trafficking in persons by any means, including the use of the internet or other information technology, and knows, suspects or ought reasonably to have known or suspected that it will be used to facilitate or promote trafficking in persons; or

(d) finances, controls or organises the commission of an offence under this Chapter, is guilty of an offence.

(2) An internet service provider operating in the Republic —

(a) must take all reasonable steps to prevent the use of its service for the hosting of information referred to in subsection (1)(c); and

(b) that has knowledge that any internet address on its server contains information referred to in subsection (1)(c) must —

(i) without delay report that internet address, as well as the particulars of the person maintaining or in any manner contributing to that internet address, to the South African Police Service;

(ii) take all reasonable steps to preserve any evidence for purposes of investigation and prosecution by the relevant authorities; and

(iii) without delay take all reasonable steps to prevent access to that internet address by any person.

(3) An internet service provider who which fails to comply with the provisions of subsection (2) is guilty of an offence.

(4)

(a) A finding by a court that an internet service provider has contravened subsection (2) serves as a ground for the revocation or cancellation of that licence.

(b) The clerk or registrar of the court which made the finding referred to in paragraph (a) must, in writing, notify the authority that granted the licence of the finding.

(c) The authority that granted the licence must review the licence and, where necessary, revoke or cancel the licence."

"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 an electronic communication service licence issued to the first-mentioned person under Chapter 3 of the Electronic Communications Act".[57]

---

[57] "Internet service provider" is defined in s1 of the Bill as meaning an "internet service provider as defined in section 1 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act No. 70 of 2002)", where the term is, in turn, defined as having the meaning set out in paragraph 0

ANNEXURE B: CHAPTER 11 OF THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT, 2002

"LIMITATION OF LIABILITY OF SERVICE PROVIDERS

70. Definition

In this Chapter, "service provider" means any person providing information system services.

71. Recognition of representative body

(1) The Minister may, on application by an industry representative body for service providers by notice in the *Gazette*, recognise such body for purposes of section 72.

(2) The Minister may only recognise a representative body referred to in subsection (1) if the Minister is satisfied that -

(a) its members 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; and

(d) the representative body is capable of monitoring and enforcing its code of conduct adequately.

72. Conditions for eligibility

The limitations on liability established by this Chapter apply to a service provider only if -

(a) the service provider is a member of the representative body referred to in section 71; and

(b) the service provider has adopted and implemented the official code of conduct of that representative body.

73. Mere conduit

(1) A service provider is not liable for providing access to or for operating facilities for information systems or transmitting, routing or storage of data messages via an information system under its control, as long as the service provider -

(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.

(2) The acts of transmission, routine and of provision of access referred to in subsection (1) include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place -

(a) for the sole purpose of carrying out the transmission in the information system;

(b) in a manner that makes it ordinarily inaccessible to anyone other than anticipated recipients; and

(c) for a period no longer than is reasonably necessary for the transmission.

(3) Notwithstanding this section, a competent court may order a service provider to terminate or prevent unlawful activity in tams of any other law.

74. Caching

(1) A service provider that transmits data provided by a recipient of the service via an information system under its control is not liable for the automatic, intermediate and temporary storage of that data, where the purpose of storing such data is to make the onward transmission of the data more efficient to other recipients of the service upon their request, as long as the service provider -

(a) does not modify the data;

(b) complies with conditions on access to the data;

(c) complies with rules regarding the updating of the data, specified in a manner widely recognised and used by industry;

(d) does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain information on the use of the data; and

(e) removes or disables access to the data it has stored upon receiving a take-down notice referred to in section 77.

(2) Notwithstanding this section, a competent court may order a service provider to terminate or prevent unlawful activity in terms of any other law.

75. Hosting

(1) A service provider that provides a service that consists of the storage of data provided by a recipient of the service, is not liable for damages arising from data stored at the request of the recipient of the service, as long as the service provider -

(a) does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of a third party; or

(b) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent; and

(c) upon receipt of a take-down notification referred to in section 77, acts expeditiously to remove or to disable access to the data.

(2) The limitations on liability established by this section do not apply to a service provider unless it has designated an agent to receive notifications of infringement and has provided through its services, including on its web sites in locations accessible to the public, the name, address, phone number and e-mail address of the agent.

(3) Notwithstanding this section, a competent court may order a service provider to terminate or prevent unlawful activity in terms of any other law.

(4) Subsection (1) does not apply when the recipient of the service is acting under the authority or the control of the service provider.

76. Information location tools

A service provider is not liable for damages incurred by a person if the service provider refers or links users to a web page containing an infringing data message or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hyperlink, where the service provider -

(a) does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of that person;

(b) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent;

(c) does not receive a financial benefit directly attributable to the infringing activity; and

(d) removes, or disables access to, the reference or link to the data message or activity within a reasonable time after being informed that the data message or the activity relating to such data message, infringes the rights of a person.

77. Take-down notification

(1) For the purposes of this Chapter, a notification of unlawful activity must be in writing, must be addressed by the complainant to the service provider or its designated agent and must include -

(a) the full names and address of the complainant;

(b) the written or electronic signature of the complainant;

(c) identification of the right that has allegedly been infringed;

(d) identification of the material or activity that is claimed to be the subject of unlawful activity;

(e) the remedial action required to be taken by the service provider in respect of the complaint;

(f) telephonic and electronic contact details, if any, of the complainant;

(g) a statement that the complainant is acting in good faith;

(h) a statement by the complainant that the information in the take-down notification is to his or her knowledge true and correct; and

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

(3) A service provider is not liable for wrongful take-down in response to a notification.

78. No general obligation to monitor

(1) When providing the services contemplated in this Chapter there is no general obligation on a service provider to -

(a) monitor the data which it transmits or stores; or

(b) actively seek facts or circumstances indicating an unlawful activity.

(2) The Minister may, subject to section 14 of the Constitution, prescribe procedures for service providers to -

(a) inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service; and

(b) to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service.

79. Savings

This Chapter does not affect -

(a) any obligation founded on an agreement;

(b) the obligation of a service provider acting as such under a licensing or other regulatory regime established by or under any law:

(c) any obligation imposed by law or by a court to remove, block or deny access to any data message; or

(d) any right to limitation of liability based on the common law or the Constitution."