Internet Service Providers' Association

queries@ispa.org.za
010 500 1200
http://www.ispa.org.za
PO Box 518, Noordwyk, 1687

30 June 2016

Department of Justice and Constitutional Development

Per email: nap@justice.gov.za

To whom it may concern

SUBMISSIONS ON THE DRAFT NATIONAL ACTION PLAN FOR COMBATING RACISM, RACIST SPEECH, XENOPHOBIA AND RELATED INTOLERANCES 2016-2021

1. ISPA refers to the draft National Action Plan to combat Racism, Racial Discrimination, Xenophobia and Related Intolerance 2016 – 2021 ("**the Draft NAP**") published by the Department of Justice and Constitutional Development ("**the Department**") for public comment, and sets out its submissions below.

About ISPA

2. ISPA was formed in 1996 as a South African Internet industry body not for gain. ISPA is now a Non Profit Company (NPC) and has a current membership of 175 large, medium and small Internet access and related service providers.

3. ISPA has played an active role in the development of electronic communications policy and legislation in South Africa. The Association has provided submissions and feedback to such key pieces of legislation as the Electronic Communications and Transactions Act, the Electronic Communications Act, the ICASA Amendment Act, and worked closely with the Department on certain aspects of the Regulation of Interception of Communications and Provision of Communicated-related Information Act.

4. Over the years, ISPA has developed good working relationships with many governmental bodies, including the Department of Communications, the Department of Telecommunications and Postal Services, SAPS, the Independent Communications Authority of South Africa (ICASA), the Film and Publications Board, the National Gambling Board and various Parliamentary Portfolio Committees.

5. ISPA has also served as an expert resource regarding electronic communications to various Government bodies and the general public.

6. Further information on ISPA and the various activities it engages in is available from www.ispa.org.za.

Scope of Submissions

7. Given its status as a representative body for Internet access and service providers, ISPA's submissions relate to those provisions of the Draft NAP relating to illegal speech where this occurs online.

8. ISPA has sought to provide constructive input on those aspects of the Draft NAP relating to the online environment and would happily engage further with the Department in this regard if this would prove useful.

Role-players in the publication of content online

9. Terminology used in the online world is vague and confusing for a lot of people, and it is critical to ensure that different role-players are clearly identified and that appropriate obligations are attached to these role-players in seeking to further the objectives of the NAP and designing proposed joint programmes and measures.

10. ISPA suggests that the Department consider the following simplified delineation:

Content providers	This refers to those who generate content and includes governments, corporations and individuals. A person who posts illegal speech on Twitter or Facebook or on a website is a content provider.
Platform providers	This refers to companies (usually) who create a platform for the hosting and publication of content from content providers. This includes Facebook, Twitter and a large number of other entities, public and private, catering for general social and niche interests.
Hosting providers	This refers to companies (usually) which operate infrastructure in the form of servers – usually located in data centres – which host websites and other forms of content available on the Internet. Telkom and Hetzner are two large hosting providers in South Africa while SITA acts as the hosting provider for government websites.
Access providers	This refers to companies which sell to consumers the ability to access the Internet and the content on it, as well as a variety of other services which operate over Internet Protocol (IP). The biggest access provider in South Africa is Vodacom through its mobile Internet services, while Telkom, MWEB and Internet Solutions are other major Internet Access Providers.
Content consumers	This refers to those who access the Internet and the content provided by content providers. Content consumers are those directly affected by illegal speech online.

11. All of these groups perform different roles and bear different responsibilities in curbing illegal speech online.

12. ISPA – as a representative body for ISPs – has made submissions in respect of the interaction between its member access and hosting providers. ISPA does not represent social media platform providers.

"Internet Service Providers"

13. The Draft NAP uses the term "Internet Service Provider", a term which is in everyday use but which describes a wide range of activities. ISPA submits that the Department may find it helpful to distinguish between Hosting providers and Access providers, as these terms are described in the table above. Both of these are generally regarded as ISPs in that they provide services related to the Internet.

14. As is set out in the discussion below regarding the treatment of "Information System Service Providers" under the Electronic Communications and Transactions Act, there are different legal considerations applicable to the provision of hosting services as opposed to access services.

"Internet Service Providers and Social Media Platforms"

15. The Draft NAP consistently refers to "Internet Service Providers and Social Media Platforms" when setting out proposed policy in respect of measures to be undertaken to address illegal speech online.

16. While both Internet Service Providers and Social Media Platforms – Platform Providers in the table above - are Internet intermediaries, they are very different in the services they provide, the manner in which they interact with their customers, and the roles they can potentially play in furthering the objectives of the NAP.

17. A social media platform such as Facebook or Twitter provides a platform for its users to publish and share information. A variety of content is made available, including advertising and the platform's own content: but the vast majority is what is referred to as User-Generated Content (UGC) in the form of posts, tweets, photographs, videos etc. The platform facilitates the publication and sharing of content and derives revenue from the sale of targeted advertising opportunities and other uses of the enormous amount of UGC published.

18. Whereas a user of a social media platform is constantly interacting with that platform, the customers of an ISP rarely have any further engagement with their ISP other than signing up for its services and paying for them.

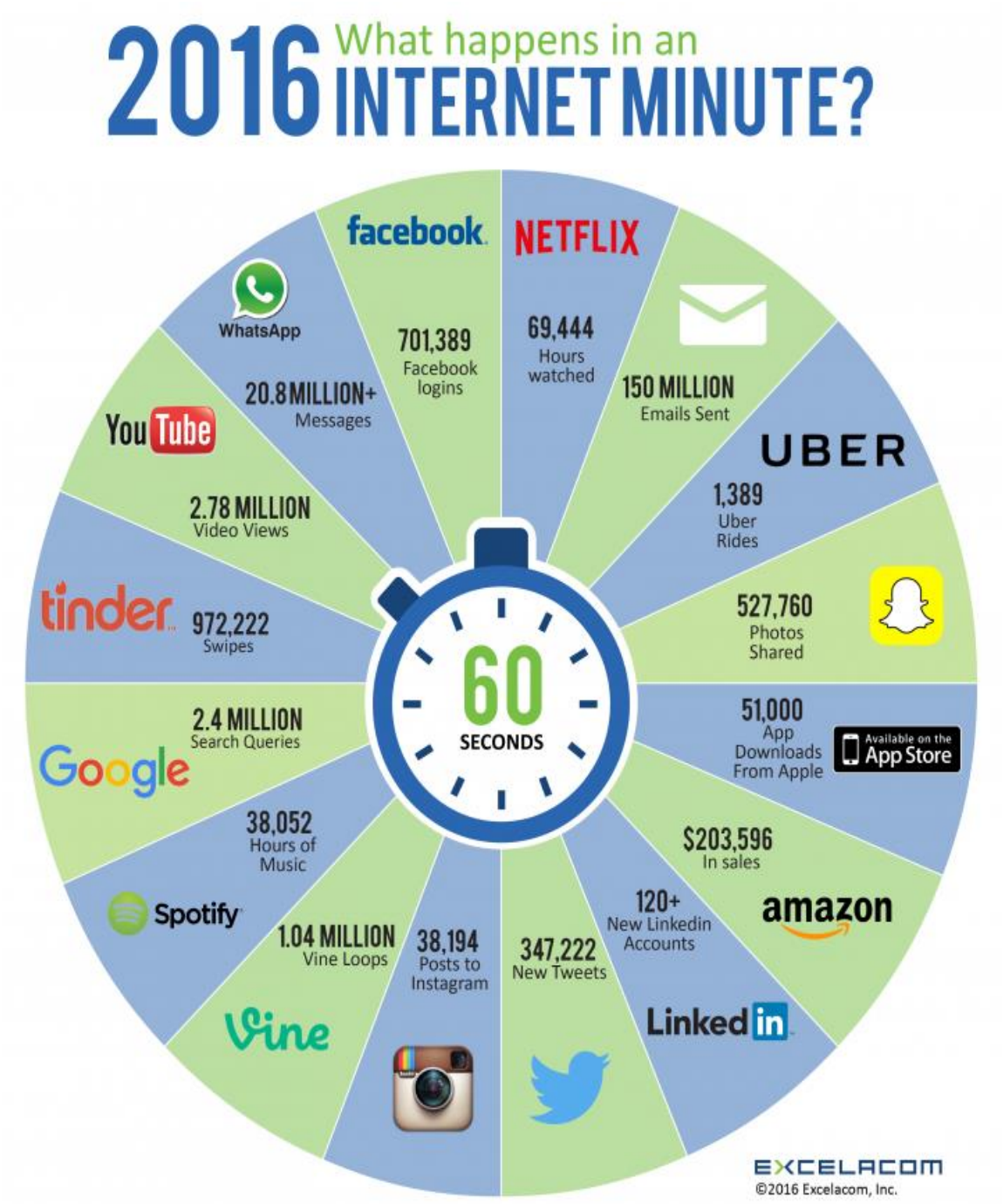
How much online content is there?

19. ISPA submits that there are two significant challenges to regulating illegal speech published or otherwise made available online:

    19.1. The borderless nature of the Internet and the difficulties of extra-territorial enforcement; and

19.2. The mind-boggling amount of content available online.

20. Both of these issues are well-known, but the graphic below – which shows how much activity occurs online in a single minute – underscores just how much content is being generated and consumed on the Internet[1]:



[1] http://www.excelacom.com/resources/blog/what-happens-in-an-internet-minute-how-to-capitalize-on-the-big-data-explosion

Position of Internet Service Providers under South African law

21. We have set out below an analysis of the framework established under the ECT Act regulating the liability of information system service providers such as ISPs.

22. One of the motivations for doing so is to demonstrate to the Department that there are already existing mechanisms in place for the expeditious removal of unlawful content online. In particular, we would ask the Department to consider the different obligations attached under the ECT Act to Internet access providers, hosting providers and other intermediaries.

23. The ECT Act includes the following definitions which make it clear that an "information system service provider"[2] is an intermediary and that an intermediary is neither a content provider nor a content consumer:

    "**intermediary**" means a person who, on behalf of another person, whether as agent or not, sends, receives or stores a particular data message or provides other services with respect to that data message;

    "**addressee**", in respect of a data message, means a person who is intended by the originator to receive the data message, but not a person acting as an intermediary in respect of that data message;

    "**originator**" means a person by whom, or on whose behalf, a data message purports to have been sent or generated prior to storage, if any, but does not include a person acting as an intermediary with respect to that data message;

24. ISPA wishes to emphasise that the ECT Act clearly distinguishes between the different roles played by content providers, content platforms and Internet Access Providers.

ISPA as an Industry Representative Body

25. The Minister of Communications (now the Minister of Telecommunications and Postal Services) formally recognised ISPA as an Industry Representative Body ("IRB") in terms of section 71 of the Electronic Communications and Transactions Act 25 of 2002 ("the ECT Act") on 20 May 2009.

---

[2] Section 70 of the ECT Act notes that, for the purposes of Chapter 11, a "service provider" means any person providing information system services. This is fleshed out by a further definition of "information system services" contained in section 1:

> **'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;

For completeness it is necessary to also mention the definition of "information system" contained in section 1:

> **'information system'** means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet;

26. The effect of formal recognition as an IRB is that ISPA's members are entitled to claim the limitations on liability in respect of content carried over their networks which are created by Chapter XI of the ECT Act.

27. Under section 71(2) of the ECT Act the Minister of Telecommunications and Postal Services may only grant such recognition to a representative body if he or she is satisfied that its members are subject to a code of conduct which requires continued adherence to prescribed standards of conduct and that the representative body is itself capable of monitoring and enforcing its code of conduct.

28. Entities falling within the definition of "service provider" set out in section 70 of the ECT Act will only be entitled to the limitations of liability set out in Chapter XI where:

    28.1. They are members of a recognised IRB; and

    28.2. They have adopted and implemented the official code of conduct of the IRB.

29. The Minister of Communications has prescribed standards of conduct to be incorporated into representative body codes of conduct through the publication of Guidelines for the Recognition of Industry Representative Bodies ("the IRB Guidelines").

30. ISPA undertook a lengthy process of amendments to its Code of Conduct and interaction with the then Department of Communications to ensure that the Code complies with the criteria set out in the IRB Guidelines. ISPA was recognised as an IRB on 20 May 2009.

31. The current version of the ISPA Code of Conduct is available at www.ispa.org.za/code-of-conduct.

Internet Access Providers act as "mere conduits"

32. Section 73 of the ECT Act stipulates that 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".

33. This immunity holds only where the service provider:

    33.1. is a member of an IRB and has adopted and implemented the code of conduct of that IRB;

    33.2. does not initiate the transmission;

    33.3. does not select the addressee;

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

    33.5. does not modify the data contained in the transmission.

34. The section 73 "mere conduit" immunity does not interfere with the right of the courts to order a service provider to terminate or prevent unlawful activity in terms of any other law which may apply.

35. In simple terms: ISPA's members, when acting in the capacity of service providers, are provided with legislative immunity from liability in respect of the content which flows over their networks subject to the provisions of the ECT Act.

36. Even where ISP's are not members of ISPA, there is other legislation – as well as the common law relating to defamation - that reinforces the "mere conduit" principle, albeit by exclusion rather than inclusion.

37. Electronic networks are nothing more than the offline equivalents of roads and railways, whilst ISP's are nothing more than the electronic version of post offices and courier companies. In other words, they are the electronic version of common carriers. In this regard, ISPA notes that there is no legal precedent that imposes liability on common carriers for the goods that are conveyed over or by them in the lawful execution of its functions and duties.

Hosting, caching and information local tools

38. This legislative immunity also covers hosting of content, caching of content and the provision of tools such as hyperlinks which are designed to assist users to find information. In all of these instances there are further requirements set out in the relevant section and which in essence stipulate that the provision of the service or performance of the activity must take place at arm's length, in accordance with industry standards and that the service provider should not have knowledge of unlawful activity.

39. Section 76(d) of the ECT Act holds that the immunity for providers of information location tools only applies where the provider "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".

Take-Down Notice Procedure

40. Section 77 of the ECT Act creates a procedure which allows a complainant to notify a service provider or its designated agent (such as ISPA) of unlawful activity in a written notice which sets out the right which has been infringed and the location or nature of the infringing material or activity under the control of the service provider.

41. A service provider is obliged to act expeditiously to remove or disable access to infringing content, failing which it may lose the immunity it has in respect of hosted content under section 75 of the ECT Act.

42. ISPA has established a Take-Down Procedure and Take-Down Guide as well as an online facility that allows for the lodging of take-down notices in respect of infringing content or activities hosted or under the control of ISPA members in their capacity as service providers[3].

[3] http://ispa.org.za/code-of-conduct/take-down-guide/

No general obligation to monitor

43. Section 78 of the ECT Act explicitly states that services providers are not under any general obligation to monitor the data which it transmits or stores or to actively seek facts or circumstances indicating an unlawful activity.

44. This is recognition of practical reality: even a small Internet access provider would find it impossible to monitor all the content flowing over its systems due to the volume of content and the speed at which it travels.

45. Internet access providers are further under a Constitutional imperative to respect the privacy of their subscribers and, as previously mentioned, are prohibited under RICA from any unauthorised interception and/or monitoring of electronic communications.

46. It is important to note that as soon as a service provider becomes aware of conduct or content which it knows to be illegal or unlawful it can no longer rely on the Chapter 11 limitations of liability.

47. While a service provider is under no obligation to monitor the data which it transmits or stores or to seek out facts or circumstances which indicate an unlawful activity, once it becomes aware of such facts or circumstances it is obligated to respond thereto with reasonable expediency.

48. This obligation to act may take a number of forms but will generally involve reporting a matter to the SAPS or Film & Publications Board, retention of evidence and/or the disabling of access or taking down of content.

Guidelines for the recognition of Industry Representative Bodies

49. As a recognised IRB, ISPA's Code of Conduct is compliant with the requirements of the Guidelines for Recognition of the Industry Representative Bodies of Information System Service Providers contemplated in Chapter XI of the ECT Act ("the IRB Regulations") as promulgated by the Minister of Communications.

50. The IRB Regulations underpin the approach of placing the emphasis for control on self-regulation by the industry rather than directly applicable legislation or government regulation and intervention.

    The only monitoring or control done by the state in the above process is to ensure that the IRB and its ISPs meet certain minimum requirements laid down in the ECT Act.

    The ECT Act is also quite emphatic that there is no general requirement on ISPs to monitor whether the recipients of the service are transgressing the law or to monitor data that it transmits or stores.

    This is simply a realistic approach, taking cognisance of economic and practical realities in the internet environment.

    This set of guidelines provides assistance to Industry Representative Bodies and ISPs on the minimum requirements regarded as adequate by the Minister and against which any application

for recognition will be measured. It also contains guidelines on what is viewed as international best practice and the standards that should ultimately be striven for.[4]

ISPs and law enforcement

51. There are further a number of Acts which include provisions which place specific obligations on ISPs or "electronic communications service providers" to assist the state with various law enforcement functions. These include:

    51.1. The Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 ("RICA");

    51.2. The Films and Publications Act 65 of 1996;

    51.3. The Protection from Harassment Act 17 of 2011; and

    51.4. The Maintenance Act 99 of 1998

52. ISPs are also subject to legislation of general application, such as the Criminal Procedure Act 51 of 1977, and legislation which empowers entities such as the South African Revenue Service (SARS) and the Financial Services Board (FSB) to request information from third parties relating to investigations falling within their jurisdiction.

53. This reflects the role of ISPs in assisting law enforcement agencies to execute their mandates. ISPs – like other intermediaries – are neutral but hold information which may be of assistance to such agencies. The balancing of the rights of privacy of the ISPs customers and law enforcement is achieved through a series of procedural safeguards set out in various pieces of legislation.

54. Requests for information targeting ISPs and telecommunications providers are a daily occurrence.

55. ISPA works closely with SAPS and other law enforcement agencies within the bounds of such legislation.

The role of Internet Service Providers in furthering the objectives of the National Action Plan

56. There are already a number of mechanisms in place regarding illegal speech online.

The ISPA Code of Conduct and IRB Guidelines

57. As set out above, ISPA members are required to adhere to the ISPA Code of Conduct, which in turn is compliant with the requirements of the IRB Guidelines.

58. Section 3 of the ISPA Code of Conduct requires members to "respect the constitutional right to freedom of speech and expression", which would include respect for the limitations on freedom of speech and expression set out in section 16 of the Constitution (i.e. that this right does not extend to propaganda for war; incitement of imminent violence; or advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm).

59. Section 8 read with section 9 of the ISPA Code of Conduct requires all members to have an Acceptable Use Policy (AUP) which is binding on their customers and which includes a requirement

[4] IRB Regulations paragraph 1

that the customer will not knowingly create, store or disseminate any illegal content and will conduct him or herself lawfully in using the service provided. In the event that the customer does not comply with this requirement the ISPA member must have the right to suspend and/or terminate service provision to that customer (see further below).

The Take-Down Notice procedure

60. The Take-Down Notice procedure set out in section 77 of the ECT Act can be used and is being used to remove illegal speech published on a locally-hosted website or platform.

61. ISPA's records indicate that it received 21 Take-Down Notices relating to Defamation, Harassment, Hate Speech and Privacy between January and the end of May 2016.

62. ISPA has established a Take-Down Guide (http://ispa.org.za/code-of-conduct/take-down-guide/) and Take-Down Procedure (http://ispa.org.za/code-of-conduct/take-down-procedure/) as well as an online facility that allows for the lodging of take-down notices in respect of infringing content or activities hosted or under the control of ISPA members in their capacity as service providers (http://ispa.org.za/code-of-conduct/request-a-take-down/).

Acceptable use policies (AUPs) and Terms and Conditions of Service

63. It is a requirement of the ISPA Code of Conduct and standard practise in the ISP industry for services to be provided subject to an Acceptable Use Policy or AUP, which sets out what categories of behaviour will and will not be permitted by users of a service.

64. It is further a condition of the provision of the service that the service provider may suspend or terminate the service if the user breaches the AUP.

65. An ISP AUP will prohibit any illegal use of the services provided, which would include use of the service to publish illegal speech.

66. We have set out below typical clauses found in an AUP:

    General: The use of our services in any way that constitutes any of the following is prohibited:

    - *a criminal act;*
    - *unlawful, incitement to commit criminal acts;*
    - *interference with the use or enjoyment of services received by others;*
    - *resulting in the publication of threatening or offensive material which is harmful, obscene, discriminatory, defamatory or constitutes hate speech; or*
    - *constitutes abuse, a security risk or a violation of privacy.*

    Unlawful Activities: Our services shall not be used in connection with any criminal, civil or administrative violation of any applicable local, provincial, national or international law, treaty, court orders, ordinance, regulation or administrative rules.

    Threatening Material or Content: Our services shall not be used to host, post, transmit, or re-transmit any content or material that harasses, or threatens the health or safety of others.

<u>Hosting services</u>: We reserve the right to decline to provide hosting services if the content is determined to be illegal or unlawful.

Knowledge of illegal speech

67. We wish to stress that the limitations on liability set out in the ECT Act are tempered by the requirement that an ISP which has knowledge of illegal speech is required to take action to report this to an appropriate law enforcement agency. Once this knowledge is present, it cannot be ignored.

68. A difficulty here is defining the point at which an ISP can be said to have knowledge that illegal speech is being hosted on its network or its services or being used for this purpose.

69. Defining what is and what is not hate speech is a notoriously difficult exercise properly in the domain of the courts: ISPs are not in any position to make such a determination and cannot be placed in the position of judging complex issues relating to exercises of the constitutional right to freedom of expression. An ISP is not a legal firm or a court of law: it should not and cannot be expected to act as such.

70. Where an ISP is presented with a court order or similar document notifying it of the hosting or distribution of illegal speech it will comply with such order immediately.

Limitations on what ISPs can do

71. It must be absolutely clear to all parties that South African ISPs are unable to take-down or otherwise deal with content which is placed on social media platforms based outside of South Africa or which is hosted outside of South Africa. Media reports indicate that the majority of illegal speech is posted on platforms such as Facebook and Twitter, but there are also smaller platforms based in jurisdictions such as Russia which have previously demonstrated the difficulties of dealing with illegal content on these platforms.

72. There is nothing local access or hosting providers can do about this material, even if they are provided with a court order notifying them that it is in fact illegal speech.

73. As regards locally-hosted content, the question must be asked as to at what stage there is knowledge that a service is being used for the dissemination of illegal speech?

Proposed Amendments to the Films and Publications Act

74. Set out below are amendments to section 27A of the Films and Publications Act 65 of 1996 proposed by the Films and Publications Amendment Bill 2016, currently before Parliament:

27A. Registration and other obligations of ~~Internet~~ internet service providers

(1) Every ~~Internet~~ internet service provider shall -

(a) register with the Board in the manner prescribed by regulations made under this Act; and

(b) take all reasonable steps to prevent the use of their services for the hosting or distribution of child pornography.

(2) If an ~~Internet~~ internet service provider has knowledge that its services are being used for the hosting or distribution of child pornography or advocating racism and hate speech, such ~~Internet~~ internet provider shall -

(a) take all reasonable steps to prevent access to the child pornography by any person;

(b) report the presence thereof, as well as the particulars of the person maintaining or hosting or distributing or in any manner contributing to such ~~Internet~~ internet address, to a police official of the South African Police Service; and

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

(3) An ~~Internet~~ internet service provider shall, upon request by the South African Police Service, furnish the particulars of users who gained or attempted to gain access to an ~~Internet~~ internet address that contains child pornography.

(4) Any person who-

(a) fails to comply with subsection (1) shall be guilty of an offence and liable, upon conviction, to a fine not exceeding R150 000 or to imprisonment for a period not exceeding six months or to both a fine and such imprisonment; or

(b) fails to comply with subsection (2) or (3) shall be guilty of an offence and liable, upon conviction, to a fine not exceeding R750 000 or to imprisonment for a period not exceeding five years or to both a fine and such imprisonment.

75. ISPA requests that the Department, in the event that it has not done so already and noting further similar provisions proposed for inclusion in draft cybercrimes legislation – consult with the Department of Communications to ensure alignment between the NAP and the Films and Publications Amendment Bill 2016.

Conclusion

76. ISPA will continue to engage with all stakeholders regarding the measures which can be taken by Internet service providers to ensure responsible and constructive use of electronic communications in South Africa.

77. In the event that the Department wishes to engage further regarding online aspects of the Draft NAP, please let us know.

PER ISPA REGULATORY ADVISORS