

# PRESS STATEMENT

FOR IMMEDIATE RELEASE

March 19, 2014

## Call for Amendment of the Anti-Pornography Act, 2014

As we celebrate 25 years of the World Wide Web (WWW) this year, we, members of the Information Communication and Technology (ICT) fraternity in Uganda strongly condemn specific sections of the Anti Pornography Act, 2014. We believe that implementation of this Act in its current form will cause a significant harm to the internet and technology ecosystem in Uganda. Specifically, those sections which constitute an infringement on the principles of the internet, namely openness and privacy.

We believe there are alternative methods of controlling the consumption of pornography by adults without necessarily compelling internet and content providers to be liable for hosting pornographic content.

We draw attention to the particular Sections 7 (f), 13, and 17 – namely:-

Section 7 (f) requires the setting up of Pornography Control Committee whose functions among others is to “expedite the development or acquisition and installation of effective protective software in electronic equipment such as computers, mobile phones and televisions for the detection and suppression of pornography.” We suggest that any software to be developed or acquired should only be to detect and suppress child pornography and this should only be implemented by Internet Service Providers (ISPs).

Section 17 (1) states, “An Internet Service Provider (ISP) who, by not using or enforcing the means or procedures recommended by the Committee to control pornography, permits to be uploaded or downloaded through its service, any content of a pornographic nature, commits an offence and is liable, on conviction, to a fine not exceeding five hundred currency points or imprisonment not exceeding five years or both.” We believe that filtering content violates the principle of net neutrality - which requires ISPs and governments to treat all data on the Internet equally, not discriminating or charging differently by user, content, site, platform, application, type of attached equipment, and modes of communication.

Section 17(1) is also a clear violation of the International Principles on the Application of Human Rights to Communications Surveillance (<https://en.necessaryandproportionate.org/text>);- Principle on the Integrity of communications and systems, which states that “In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State surveillance purposes. A priori data retention or collection should never be required of service providers. Individuals have the right to express themselves anonymously; States should therefore refrain from compelling the identification of users as a precondition for service provision.”



Also, in order to avoid infringing internet user's rights to freedom of expression and right to privacy, ISPs should only implement restrictions to these rights after judicial intervention. ISPs should be transparent to their customers about the measures to be taken should they receive a takedown directive and they should minimize the impact of any restrictions to the specific content involved.

Meanwhile, Section 13 (1) which states that "A person shall not produce, traffic in, publish, broadcast, procure, import, export, sell or abet any pornography" also violates adult users' rights to access information and right to conscience.

We also observe that the conviction of the offence of Child Pornography as provided in Section 14 Subsection (1) contradicts that provided in The Computer Misuse Act, 2011, Section 23 Subsection (4). According to this Act, Section 14 (1) states that 'A person who produces, participates in the production of, traffics in, publishes, broadcasts, procures, imports, exports or in any way abets pornography depicting images of children, commits an offence and is liable on conviction to a fine not exceeding seven hundred and fifty currency points or imprisonment not exceeding fifteen years or both.' Whereas under the Computer Misuse Act, 2011, a person who commits an offence of child pornography is liable on conviction to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

We therefore recommended that:

1. A clearer distinction between the different forms of pornography should be made. Whereas the Act defines Child pornography, there is a need to add to the definition of "pornography" the different forms of pornography to include: Softcore pornography (contains nudity or partial nudity in sexually suggestive situations, but not explicit sexual activity, sexual penetration) and hardcore pornography (contains graphic sexual activity and visible penetration). Specific guidelines need to be developed for the consumption of Softcore pornography especially in public places.
2. ISPs and Internet content providers should be liable for removing illegal content hosted on their networks/systems but should NOT be liable for the content that merely flows through their networks. The only liability should be placed on internet content developers, publishers or broadcasters who allow for hardcore pornography to be published to the public. Also liability should be placed on the user who consumes pornography in the public domain.
3. The Act should be amended to clearly state the procedures and measures to be taken by the Pornography Control Committee against ISPs and other content hosts to control pornography consumption in the public. A mere development or acquisition and installation of effective protective software in electronic equipment such as computers, mobile phones and televisions for the detection and suppression of pornography as stated in Section 7 (f) does not provide definite steps on how the software will function or suppress pornography.
4. Section 7 (f) should be amended to only cover the development or acquisition and installation of effective software in electronic equipments to detect or suppress child pornography by ISPs.
5. Section 13 (a) should be changed to reflect prohibitions on pornography production, publishing, broadcasting only in public places. People should be allowed to procure pornography as long as it is watched within restricted areas such as residential places.
6. Section 13 (a) should be split to address child pornography and adult pornography separately:
  - Section 13 (a): A person shall not produce, publish, broadcast, procure, sell or abet any form of

hardcore pornography in public places.

- Section 13 (b): A person shall not produce, traffic in, publish, broadcast, procure, import, export, sell or abet any form of child pornography.
7. Section 13 (2), which provides for punishment of five hundred currency points or ten years imprisonment or both should be shifted to perpetrators of hardcore pornography in public places.
  8. In line with the proposed amendment of Section 13(a), a definition of “public places” should be stated in the Act.
  9. Section 14 should be amended to harmonise fines for conviction of child pornography with those in the Computer Misuse Act, 2011.

Lastly, we recommend that a call for wider consultation with stakeholders in making Amendments to the Act as proposed by this submission is done.

**For more information:**

**Contact**

Lillian Nalwoga  
Internet Society – Uganda Chapter  
Tel: +256712204335  
Email: [lillian@isoc.ug](mailto:lillian@isoc.ug)

