INPUTS WITH REGARDS TO CHILD ONLINE PROTECTION

The following are in line with the ITU policy actions:

1. **Law enforcement**

   The existing Mauritian legal framework has been reviewed to ensure that all necessary powers exist to enable and assist law enforcement and other relevant actors in cybercrime matters. The new Cybersecurity and Cybercrime Bill 2021 caters for cybercrime targeting children, such as misuse of fake profiles, cyberbullying, cyber extortion, amongst others.

   Moreover, with respect to fight and prevent child sexual abuse (CSA) online, the Information and Communication Technologies Authority (ICTA) has adopted a filtering solution, based on international partnership and using the method of blacklisting.

   Pursuant to Sections 18(1)(m) and (n) of the ICT Act 2001, as amended, the Authority is empowered to "*take steps to regulate or curtail harmful and illegal content on Internet and other information and communication services*" and "*ensure the safety and quality of any information and communication services*". This provision of the ICT Act 2001 is also congruent with Section 251 "*Debauching youth*" of the Criminal Code Act 1838, Section 14 "Sexual Offences" of the Child Protection Act 1995 and Section 21 "*Pornography*" of the Children's Act 2020 which criminalize the sexual offences perpetrated on children.

   The ICTA's project on CSAM filtering is also pursuant to the recommendations of the UN Committee on the Rights of the Child. In its 2014 report on "Digital media and children's rights", the UN Committee on the Rights of the Child has called on regulatory agencies to demonstrate responsibility in developing standards relevant to children's rights and ICTs.

2. **National awareness and capacity**

   Sensitization campaigns covering present Internet Dangers such as cyberbullying, sexing, sextortion and online predators / pedophiles are conducted regularly in schools throughout the island. Moreover, the Safer Internet Day is organized each year to promote a safer Internet usage amongst youngsters. Guidelines on pertinent issues related to child online safety are published every year on the CERT-MU website. Awareness programmes on cybersecurity issues are also conducted on television and radio, focusing not only on the youth but also on citizens of all age groups.

3. **Education**

   Alongside sensitization campaigns for children, awareness sessions are also organized for educators, using a "train the trainer" approach so that they can in turn communicate their knowledge to their students. In this way, both students and educators are well equipped to identify online dangers and can fully understand the implications of their online behavior.

4. Reporting

The CERT-MU has put in place the Mauritian Cybercrime Online Reporting System (MAUCORS) since 2018, which is an online complaint mechanism, with a complete set of protection guidelines for individuals, including children, to easily report cyber incidents occurring on social media as well as other cybercrimes.

The Child Sexual Abuse (CSA) filtering mechanism was launched by the ICTA in February 2011. It filters access to Child Sexual Abuse (CSA) sites for Internet users in the Republic of Mauritius. It involves the use of the Internet Watch Foundation (IWF) database, which backlists such websites or web pages and contains two aspects: (a) the reporting through the IWF portal and (b) the filtering system through the NetClean Whitebox technology.

a) The reporting system through IWF portal

A Memorandum of Understanding (MoU) was signed between IWF and ICTA on 24 October 2013 for a duration of two years. Its objective was to enable Internet users in the Republic of Mauritius to report suspected illegal CSAM hosted anywhere in the world via the dedicated platform of IWF, the Online Child Sexual Abuse Reporting Portal (OCSARP).

The mechanism comprised the linking of the IWF blacklist with local Internet Service Providers in the Republic of Mauritius via the ICTA website. Under this MoU (2013-2015), the IWF worked in partnership with ICTA to provide a reporting portal available via the ICTA website (www.icta.mu) for individuals or organisations to report potential CSAM. It assessed the online material and assisted the service providers to avoid abuse of their systems by distributors of CSAM. Even if some of the material remains available online, it is included on the IWF blacklist and blocked to stop inadvertent exposure. Even after the expiry of the MoU, ICTA kept using the IWF blacklist for its filtering system.

b) The filtering system: the NetClean Whitebox technology

The CSAM filtering mechanism set up by the ICTA makes use of the IWF database, which is updated daily and blacklists the CSAM websites or pages, preventing them from being accessed by Internet users in the Republic of Mauritius. The Child Sexual Abuse filtering system is linked with all local Internet Service Providers licensed by the ICT Authority.

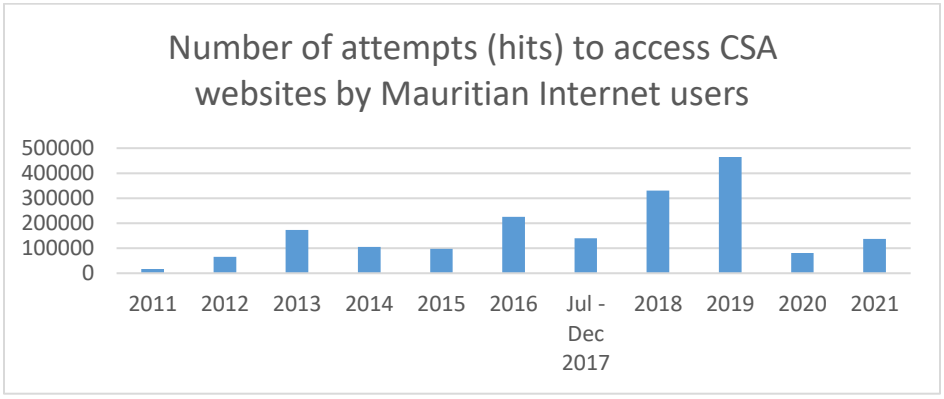
The centralised filtering system serves as a cyber security infrastructure shared among ISPs and managed by the ICTA. Once IWF adds any website or web page to its black list, the ICTA's filtering system is automatically updated so that the newly added websites or web pages can no longer be accessed to from Mauritius. Therefore, even when the removal of offensive content cannot be performed at the source, the filtering system ensures that it can no longer be viewed from Mauritius.

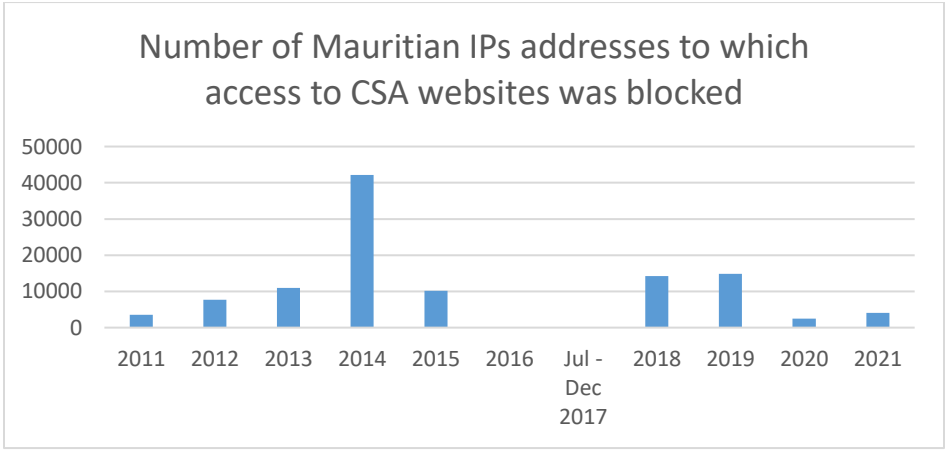
To implement this centralised filtering solution, the ICTA has been using the NetClean Whitebox technology developed specifically for the task of detecting and blocking child sexual abuse material on computer devices.

From 2011 to 2014, the CSA filtering set up was hosted at the ICTA and was connected to all local ISPs providing Internet access to the public in Mauritius. After 2014, it shifted to a cloud-based mode whereby no hardware was required anymore at the ICTA premises. Since November 2020, Netsweeper has been the new provider for CSA filtering, using the same cloud-based technology as before.

With the implementation of this CSA filtering solution, the ICTA is ensuring that ISPs are supplying their customers with an Internet connection which is clean from access to CSA websites, in the same way that a water company makes sure that the water provided in its pipes is uncontaminated. It has to be noted that the ICTA's CSAM filtering system only works for unencrypted online content (http) and does not work for encrypted content (https).

This Online Content Filtering (OCF) solution implemented by ICTA has allowed the filtering of 1,835,064 attempts (hits) to access CSA websites by Mauritian users and the blocking of 110,026 Mauritian IPs addresses since the implementation of the system in 2011.





Source: https://www.icta.mu/observatory-csa/

****