# *A FILTERING SYSTEM TO PREVENT ACCESS TO CHILD SEXUAL ABUSE MATERIAL ON THE INTERNET*

**Policy Paper**
**Advised by the Attorney General's Office, the Office of the Regulator and the National Prosecution Office**
**Submitted March 2016**

## TABLE OF CONTENTS

## 1.0 SUMMARY

The Honourable Prime Minister of Samoa asked the Office of Attorney General ("**AGO**") and the Office of the Regulator ("**OOTR**") to examine effective means of policing"*indecent material to come through the internet of which includes child sexual abuse material ("CSAM")*". This Paper concentrates on examination of effective means of policing child sexual abuse material over the internet. The narrow focus of this paper is based on consultation with the relevant authority in New Zealand who had undertaken similar projects of effectively policing CSAM over the internet. The study showed that a more narrow focus on the priority area of CSAM which is already illegal in most countries, including Samoa, produces more effective policing of indecent material on children over the internet. A wider approach results in ineffective filtering through the internet as well as continuous legal arguments of "*what is indecent material*". The working group established to examine this problem and produce a practical and workable solution decided that the best course of action is to focus the approach on policing CSAM over the internet.

The AGO, in meeting with the OOTR and the National Prosecution Office ("**NPO**"), identified three potential solutions of which are to be assessed in this Paper. The first is the amendment of the Crimes Act 2013 to criminalise Internet Service Providers ("**ISP**") who allow their users to access CSAM through the internet. The second is an amendment to the Telecommunications Act 2005, including regulations as well as a licensing regime for ISPs to conduct the policing of CSAM themselves through a filtering system operated by each ISP. The third is a government based filtering system that all ISPs must use when providing access to the internet.

In assessing these options, a workinggroup was established comprising the AGO, NPO, OOTR, Ministry of Communication and Information Technology, Ministry of Women Community and Social Development, Ministry of Education Sports and Culture, Ministry of Justice and Courts Administration, Ministry of Police, and the Pacific Transnational Crime Unit. Consultation was undertaken with the New Zealand Internal Affairs Censorship Unit andISPs. The New Zealand authority focuses on policing CSAM over the internet.

ThisPaper examines how access to CSAM on the internet can be prohibited, provides recommended options to be implemented in Samoa, and outlines the required amendments to legislation and regulations to achieve those options. It also recommended a pilot project as a first step to test out the problems, benefits and disadvantages that can be addressed.

## 2.0OBJECTIVE

The issue of access to CSAMon the internet is a growing concern that has been acknowledged in international fora and political agendas, and is now being echoed by Samoa due to the speed of which local residents have adopted and adapted to internet usage.

The deficiency in support, awareness and education for the public on being digital citizens has resulted in the negative utilisation of technology, such as children subjecting themselves or their peers to online exploitation, evidenced by a number of cases in our courts and reported by the media; but more disturbing are the adults who prey on the young digital citizens through CSAM.

In light of the situation above, it is essential to implement a filtering system as a form of response to combat the exploitation of children through the means of distributing and accessing CSAM on the internet.

## 3.0DISCUSSIONS OF THE THREE OPTIONS

### *3.1 Option One –Amendment of the Crimes Act 2013*

The first option that was discussed was the amendment of the Crimes Act 2013 to have ISPs criminally liable for its users accessing CSAM on the internet. The issue raised in that discussion is that ISPs would not have the "*required knowledge*" for prosecution under that offending. The resources required for an ISP to monitor its customers use of the internet would be very high, and potentially impossible for ISPs to achieve. Even if an ISP could monitor all of its internet traffic, it would only be able to determine which "*user account*" accessed a website with CSAM, and not the actual person using the device. There is also the privacy consideration that comes with ISPs monitoring the internet usage of its customers.

### *3.2 Option Two – Filtering by the Internet Service Providers*

Internet content may be controlled by using software packages and technical tools to censor or filter what is accessible to a user. Option Two is for ISPs in Samoa to use their own filtering systems to block access to CSAM.

The filtering system would be applied to all customersas a mandatory system, meaning that customers would not be given the ability to opt-out of using the filter, thereby covering all internet users in Samoa. This would be achieved by an amendment to the Telecommunications Act and regulations including a condition for ISPs to operate a filtering system to block CSAM as a condition of the ISP's licence.

An ISP can block or filter content at the network level using software, Domain Name System servers or firewalls with the effect of restricting its customer's access to a portion of the internet. Samoa currently has 4 ISPs, namely *Digicel (Samoa) Limited*, *Bluesky Samoa Ltd*, *Computer Services Ltd* and *Lesa's Telephone Services Ltd* (internet provided through Lesamoa.Net) and potential a fifth ISP, namely, *Netvo Samoa Ltd*, which is expected to commence operations in the near future. All of the above ISPs have confirmed they can provide a filtering system to block CSAM.

There are concerns with using ISP filtering systems for this purpose, and a number of key issues were raised during consultations with the New Zealand Internal Affairs Censorship Unit on this topic, namely:

a) if all 5 ISPs apply their own filtering system, there is a potential for 5 different kinds of filtering systems to be operating within Samoa, which could cause a significant slow-down in internet speeds. This in turn could lead to complaints from customers against their ISPs;
b) it will increase the cost to the users;
c) as the filtering system is implemented and operated by private companies, there is less control over the effectiveness and quality of filtering system used.

### *3.3 Option Three - Filtering at a national level*

At the national level, the Government can establish a national filtering system to be used by all ISPs in Samoa. The system would be implemented by establishing infrastructure to operate a centralised filtering system to block CSAM, and requiring all ISPs to use the system when providing internet access to customers. The advantage of the system is a central and uniform filtering system that would apply to all internet users in Samoa. The primary concern is how the infrastructure and operational costs for the system will be funded. Additionally, ISPs have raised concerns with using a national system,as different interconnection methods used by ISPs may lead to compatibility issues with the national filtering system.

The New Zealand Ministry of Internal Affairs is willing to assist in the training of relevant personnel for the establishment of such a unit. However, the costing will be borne by Samoa. It will have to be housed in the Office of the Regulator with a staff of about 2 people, a server and a sophisticated filtering programme to be purchased from Switzerland. The costing budget would most likely be in the range of more than $200,000.00 to establish a filtering at a national level.

## 4.0 RECOMMENDED FILTERING SYSTEM FOR SAMOA

It is recommended that Option 2 be implemented to block access to CSAM in Samoa. The recommendation is based on the advice received from ISPs in a consultation session on 23 March 2016 that the preferred method is for them to each have their own filtering system. That will benefit the Government in not needing to establish or maintain additional infrastructure to provide a national filtering service.

### *4.1 List of websites to filter*

It will be necessary to provide ISPs with a list of websites to filter ("**List**"). It is recommended that the OOTR, as the regulatory body, be responsible for developing and maintaining the List.

The List will initially be created by adopting lists already maintained by international partner organisations such as, Interpol's Worst Of List,New Zealand's Censorship Office and any other Regulatory authority able to assist (it will be necessary to seek the permission of these organisations to acquire their lists as they are maintained confidentially).It will be a requirement that the List is kept confidential at all times by the OOTR and ISPs.

The List can be reviewed every three months by a committee appointed to review it, comprised of the Regulator, The Commissioner of Police and the Director of the National Prosecution Office. The List will be reviewed by considering updates to international partner organisation lists, intelligence obtained through police operations, and reports of illegal content by members of the public. The review committee will also provide an accountability function to ensure the List only contains websites that hosts content which satisfies the definition of CSAM.

### *4.2 Landing Page*

While ISPs will use their own filtering systems to block access to the List, it is recommended that a standardised landing pagebe provided by all ISPs. A landing page is the web page that a user is redirected to when their request to access a website is blocked by the filtering system, and is designed to achieve the following:

a) informs the user that he or she has been prevented from accessing the requested website as it is used for the distribution of CSAM;
b) provides the user with a method to appeal the block; and
c) provides the user with a link to OOTR's (as the relevant regulatory authority) website, where additional information can be found about the operation of the filtering system.

### *4.3 Appeal Process*

In situations where a person is blocked from accessing a legitimate website, it is proposed an appeal process is provided to enable a person to inform the OOTR that the website they are attempting to access has been blocked in error.

This can be done through the landing page which will providethe user with an appeal form to complete and submit electronically to the OOTR. The Appeal is then reviewed by theOOTRand a decision is made to either continue blocking or remove the website from the List.

### *4.4 What if an ISP does not block access to a website on the List?*

It will be necessary to give the OOTR (as the regulatory body) the power to monitor and enforce ISP filtering of the List. If it is found that an ISP has not blocked access to a website on the List, either intentionally or due to the ineffectiveness of their filter, then the OOTR must be empowered to require the ISP to correct their filtering system to block access.

It is proposed to empower the Regulator to first issue a remedial notice allowing an ISP to block access.

The failure to comply with a remedial notice will then become an offence. However, an administrative penalty regime will be the first option, where the OOTR will issue to the ISP an infringement notice with an administrative penalty when an ISP commits the

offence. The ISP can then admit allegation in the infringement notice and pay the administrative penalty or defend the notice in court.

It is important that careful consideration is given to the wording of the ISPs obligation to provide the filtering system, and their liability if a user can access a website on the List. This is because there will always be techniques available for a user to circumvent filtering systems, and it is not reasonable to make an ISP liable for a user accessing CSAM, if the user is circumventing the filter, for example by using a proxy server or virtual private network.Therefore it is recommended that ISPs will not be liable for access to websites on the List, in the event that a user circumvents the ISPs filtering system to access the banned website.

## 5.0LEGAL MEASURES

To implement Option 2 the following amendments or actions are considered necessary(proposed amendments are to be made to the*Telecommunications Act 2005* ("the Act")):

### *5.1 Definition of CSAM*

In order to determine what content a potential filtering system would block on the internet, it is important to develop a clear definition of CSAM. This definition will govern what websites must be blocked and ensure that all stakeholders are clear as to what content constitutes CSAM.

Our proposed legislative amendment to the Act will provide the definition of CSAM as follows:

> *Child Sexual Abuse Material* is material that:
> (a) promotes or supports, or tends to promote or support, the exploitation of children for sexual purposes and includes material that depicts sexual conduct with or by children; or
> (b) exploits the nudity of children; and
> (c) includes any film, image, document, audio, or computer generated material.

### *5.2 Power for Regulator to create and maintain the List*

A legislative amendment should be inserted in the Actto give the Regulator the ability toestablish and maintain a list of websites that are deemed to host Child Sexual Abuse Material in consultation with the Commissioner of Police and the Director of National Prosecutions.

### *5.3 Requirement for ISPs to provide filtering system*

A legislative amendment should be inserted in the Act to: require ISPs to provide a filtering system to block access to websites on the list created by the Regulator in item 5.2 above. The amendment must include an exception where customers bypass an ISPs

filtering system to access a website on the List (for example by proxy server or virtual private network.).

This amendment should include an exemption provision that allows certain ministries or organisations to have the filtering system disabled for their internet service, in the event they need to access websites on the List for a lawful purpose. This could include situations where the police or NPO need to access a banned website for the purpose of prosecution.

### *5.4 Remedies for failing to provide filtering system*

A legislative amendment should be inserted in the Act to provide a remedy for ISPs failing to provide a filtering system that blocks access to websites on the List. It is proposed that the amendment will provide the Regulator the power to issue infringement notice explained in paragraphs 2 and 3 of item 4.4 above.

### *5.5 Six months trial (pilot scheme)*

It is proposed that we implement a pilot scheme that will run for a period of 6 months. Such scheme will allow us to determine the effectiveness of the filtering system and assess whether there are any compatibility issues affiliated with Option 2. It is important to test the effectiveness of the filtering system under option 2 so that we can also identify other areas of our laws that may also need to be explored in terms of possible amendments.

The pilot scheme involves the ISP providers voluntarily applying their filtering system compulsorily on their users to block the listed website from the Regulator for a period of six months. This will enable the working group to determine whether the concerns raised by the consultation with the New Zealand authority on having five different filtering systems operating in Samoa could result in drastically slowing down the internet or crash the internet. The6 months period would also allow the working group to examine available options in obtaining funds via aid in the establishment of a national filtering system. The 6 months period would also allow for the working group to bring in a member of the New Zealand authority who is an expert on filtering systems to examine the ISP providers filtering system as well as determine the compatibility issues identified by the ISP providers.

However, the proposed amendment to the Act will be developed and pursued during the pilot period, so that at the end of the pilot period the necessary amendments for a permanent solution would have already been completed.

### *5.6 Proposed amendments to ISP Licensing*

It is proposed that the requirement to provide a filtering system to block access to websites on the List is also inserted as a condition of ISPs licences.

### *5.7 Guidelines*

It will be beneficial to develop guidelines that detail how an ISP should provide a filtering system to prevent access to websites on the List. That will provide clarity on the practical implementation of the above amendments.

## 6.0EDUCATION AND PUBLIC AWARENESS

The OOTR will work with ISPs and other relevant stakeholders to promote child online safety and raise awareness of the issues with access toCSAM on the internet so that the public, and specifically children and parents, are better informed as digital citizens.

It is important that resources are dedicated to providing education and public awareness to the public, together with the technical measures outlined in this paper, to ensure a holistic response is provided for this issue.