Judge Stein Schjolberg

Proposal for a draft United Nations Treaty on combating online child sexual abuse

Peace and Justice in Cyberspace

Chairman, High Level Experts Group (HLEG), ITU, Geneva, (2007-2008)
Chair, EastWest Institute (EWI) Cybercrime Legal Working Group, (2010-2013)
Chair, The Global Think Tank on Justice, Peace and Security in Cyberspace (2013-)

stein.schjolberg@cybercrimelaw.net
www.cybercrimelaw.net

"There can be no peace without justice, no justice without law and no meaningful law without a Court to decide what is just and lawful under any given circumstances."

Benjamin B. Ferencz, Former US Prosecutor

Draft United Nations Treaty on combating online child sexual abuse
(8th Edition, June 2015)

by Judge Stein Schjolberg
www.cybercrimelaw.net

Introduction

Recalling the 1989 United Nations Convention on the Rights of the Child. Online child sexual abuse constitutes serious violations of fundemental rights, in particular of the rights of children to the protection and care necessary for their well-being.

Recalling the 2000 United Nations Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.

Noting that Article 34 of the United Nations Convention on the Rights of the Child, States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse.

Noting that online child sexual abuse are increasing and spreading through the use of new technology and the Internet, and require a comprehensive approach on the prevention of such abuses.

Recognizing with appreciation the work on the CIRCAMP (Cospol Internet Related Child Abusive Material Project) network.

Recognizing with apprecipation the work of INTERPOL providing and updating the national offices of INTERPOL with a Worst of list of domains (IWOL), including a service for Access Service Providers (ASP).

Recognizing with appreciation Directive 2011/93/EU of the European Parliament and of the Council of December 13, 2011, on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

Recalling that important initiatives was taken by the work on the CIRCAMP (COSPOL Internet Related Child Abusive Material Project) network that was launched in 2004. COSPOL is an abbreviation for: Comprehensive Operational Strategic Planning for the Police. CIRCAMP was organized by Norway and United Kingdom, and had 14 national police forces as members in addition operational support from Europol and INTERPOL. The primary goal for CIRCAMP was *"to detect, disrupt and dismantle networks, organizations or structures used for the production and/or distribution of child abusive files and to detect offenders, identity children and stop abuses."* Another initiative was an Australian based Virtual Task

Force, an alliance of international law enforcement agencies and private sector partners.

Noting that INTERPOL was a member of CIRCAMP, providing and updating the national offices of INTERPOL with a Worst of list of domains (IWOL) that was introduced in 2010.
INTERPOL has taken responsibility of providing a list of domains containing child sexual abuse content to any Internet Access Service Providers (ASP) willing to participate in reducing the availability of such material on the Web. Participation is free of charge on completely voluntary.

The criteria of being to INTERPOL ”Worst of” list are very strict and includes as follows:

- *The children are ”real”. Sites containing only computer generated, morphed, drawn or pseudo images are not included;*
- *The ages of the children depicted in sexual exploitative situations are (or appear to be) younger than 13 years;*
- *The abuses are considered severe by depicting sexual contacts or focus on the genital or anal region of the child;*
- *The domains have been online within last three months;*
- *The domains have been reviewed and found to fulfill the above criteria by two independent countries/agencies or more.*

A Stop Page was introdused and had content as follows:
” Your browser has tried to contact a domain that is distributing child sexual abuse material. Access to this domain has been blocked by your Access Service Provider in co-operation with INTERPOL.
This is a preventive measure to protect the children that have been victims of documented sexual abuse and to prevent further dissemination of the evidence of this abuse.
All domains that experience redirection have been checked by police officers at INTERPOL in co-operation with CIRCAMP, and were found to contain child sexual material according to very strict criteria.
The content on the domain may change over time and/or be hidden from plain view, so that the domain may appear legal if accessed. If you strongly believe that the domain is wrongly blocked, you may contact INTERPOL.
If you are the domain owner, you may complain about the inclusion of your domain on the list via EUROPOL.
If you would like to report content that you have come across on the Internet or use your local hotline, go to INHOPE for an overview of national hotlines in many countries.”

Noting that Google and Microsoft Bing from November 2013 adjusted their such result to block child sexual abuse content through their search engines around the world.

The model legal framework for this proposal is the Directive 2011/92/EU of the European Parliament and of the Council of December 13, 2011, on combating the sexual abuse and sexual exploitation of children and child pornography

Article 1
Subject matter

This treaty or agreement establishes minimum rules concerning preventing websites containing online child sexual abuse. It introduce blocking technology, filtering technology, or similar technology as measures aimed at stopping the distribution of child abusive images and material. When the term ”blocking” is used in this proposal it also includes ”filtering”.

Blocking websites containing child sexual abuse could be based on various types of public action, such as legislative, non-legislative, judicial or other. Voluntary actions taken by the Internet industry to prevent the misuse of its services with child sexual abuse are supported. States must ensure that it provides an adequate level of legal certainty and predictability to service providers (ISPs) and users.

Article 2
Definitions

Online child sexual abuse includes:

- any material that visually depicts a child engaged in real or simulated sexually explicit conduct, governed by national standards pertaining to the classification of materials. Text materials having an artistic, medical, scientific or similar merit may not to be sexually explicit conducts.
- any depiction of the sexual organs of a child for primarily sexual purposes, and exploited with or without the childs knowledge,
- realistic images of a child engaged in sexually explitcit conduct, or realistic images of the sexual organs of a child, for primarily sexual purposes.

Article 3
Prevention

States shall prevent deliberate access to child abuse material on the Internet, and prevent accidental access to this illegal and harmful content by the public.

States shall take appropriate preventive actions to detect, disrupt, and dismantle networks, organizations, or structures used for the production, distribution of child abusive files, and to detect offenders, identify children and stop material.

Article 4
Investigation

1.The police are responsible for confirming the illegality of the domain and to provide the addresses containing child abuse material.
The access blocking methodology targeting web domains, and web domains only, disseminating child sexual abusive files.
Blocking access to child sexual abuse files are cheap and simple preventive methods.

2. All domains are downloaded by the police, seized, traced, and looked up, saved and rechecked at predetermined intervals.

3. States that have access blocking system in place may share all information on continuously updated list on illegal sites between them, and check the content according to national legislation.

Article 5
Access blocking systems

Internet Service Providers (ISP) implements the access blocking in their networks, utilizing existing technology, personel and equipment.

1. The ISP redirects the browser to a specific page instead of the address - the socalled STOP page. The STOP page will explain the reason for the redirection of traffic, give links to legislation and police

2. The access blocking is purely preventive, no investigations against persons are initiated as a result of an Internet user being blocked and the Stop Page displayed.

3. The IP-address of the Internet users has been removed from the logs, so they contain no identifying information. Identifiable information about the Internet user is not stored.

4. The nature of the Internet makes circumvention of any blocking system possible for technically skilled people, but this does not undermine the importance of the blocking. Deliberate access may not be prevented by web blocking.

5. The Child Sexual Abuse Anti Distribution Filter (CSAADF) focuses on blocking on domain level. The blocking will not be lifted until the material is removed.

6. In cases where a hosting company has been taken advantage of, like free photo hosting companies, the owner/administrator shall be informed that they are hosting child sexual abuse material.

7. In some countries sites that provide payment services to the distributors of child abuse materiel may be blocked.

Article 6
Measures against websites containing or disseminating online child sexual abuse

1. States shall take measures to block access to websites containing online child sexual abuse.

2. States may take measures to block access to websites containing online child sexual abuse, including children between 13 and 18 years.

3. The removal of webpages and blocking of websites shall be directed towards the Internet users within the territory of the individual State.

The measures must be set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction.

Article 7
INTERPOL

The global police organization INTERPOL shall provide a Worst of list of domains (IWOL) for the prevention of child sexual abuses, that contains domains evaluated and found to be online and distributing child sexual abuse material.
Included in the list shall be domains that contains images and/or movies which fit the following criteria:

1. The children are ”real”. Sites containing only computer generated, morphed, drawn or pseudo images are not included.

2. The ages of the children depicted in sexually exploitative situations are, or appears to be younger than 13 years.

3. The abuses are considered severe by depicting sexual contact or focus on the genital or anal region of the child.

4. The domains have been online within last three months.

5. The domains have been reviewed and found to fulfill the above criteria by two independent countries/agencies or more.

INTERPOL shall provide ASP/ISP and other providers of services on the Internet with the IWOL list of domains containing child sexual abuse material.

Article 8
Review Board

A Review Board shall be established, including members from the relevant United Nations institutions and INTERPOL.

Article 9
Annual report

The Review Board shall annually submit a report to the United Nation General Assembly, assessing the extent to which States have taken the necessary measures in order to comply with this treaty or agreement, accompanied if necessary by legislative proposals.