

ONLINE CHILD SEXUAL EXPLOITATION

A COMMON UNDERSTANDING

A user-friendly booklet on the manifestations, legal frameworks and technical terms and tools related to online child sexual exploitation



ECPAT International is a global network of civil society organisations working together to end the sexual exploitation of children (SEC) including the exploitation of children through prostitution, child sexual abuse material, trafficking of children for sexual purposes and the sexual exploitation of children in travel and tourism. It seeks to ensure that children everywhere enjoy their fundamental rights free and secure from all forms of sexual exploitation.

The ECPAT International network currently has 95 member organisations in 86 countries. ECPAT Member Groups are involved in the implementation of various initiatives to protect children at local and national levels, while the ECPAT Secretariat (based in Bangkok, Thailand) provides technical support, research and information. It also represents and advocates on key issues in international and regional fora on behalf of the network.

This publication was made possible with the generous financial support of Terre des Hommes the Netherlands.



The factsheets were developed by the Programme Combating Sexual Exploitation of Children Online at ECPAT International.

Support for translation and production of the Manifestations factsheets and the Internet and Technology factsheets in Burmese, Indonesian (Bahasa), Khmer, Lao, Thai and Vietnamese was provided by the UNICEF Regional Office for East Asia and the Pacific, with kind assistance from ECPAT Member groups and other civil society organisations in the respective countries.

We acknowledge our core funders Sida and Oak Foundation for their ongoing support to the work of ECPAT International

May 2017, Copyright © ECPAT International 2017

Written by: Yvonne Nouwen

Design and layout by: Manida Naebklang

Additional credits: Marie-Laure Lemineur, Rangsim Deesawade, Thomas Muller, John Carr.

Published by:

ECPAT International

328/1 Phaya Thai Road, Ratchathewi, Bangkok 10400 Thailand

Tel: +662 215 3388

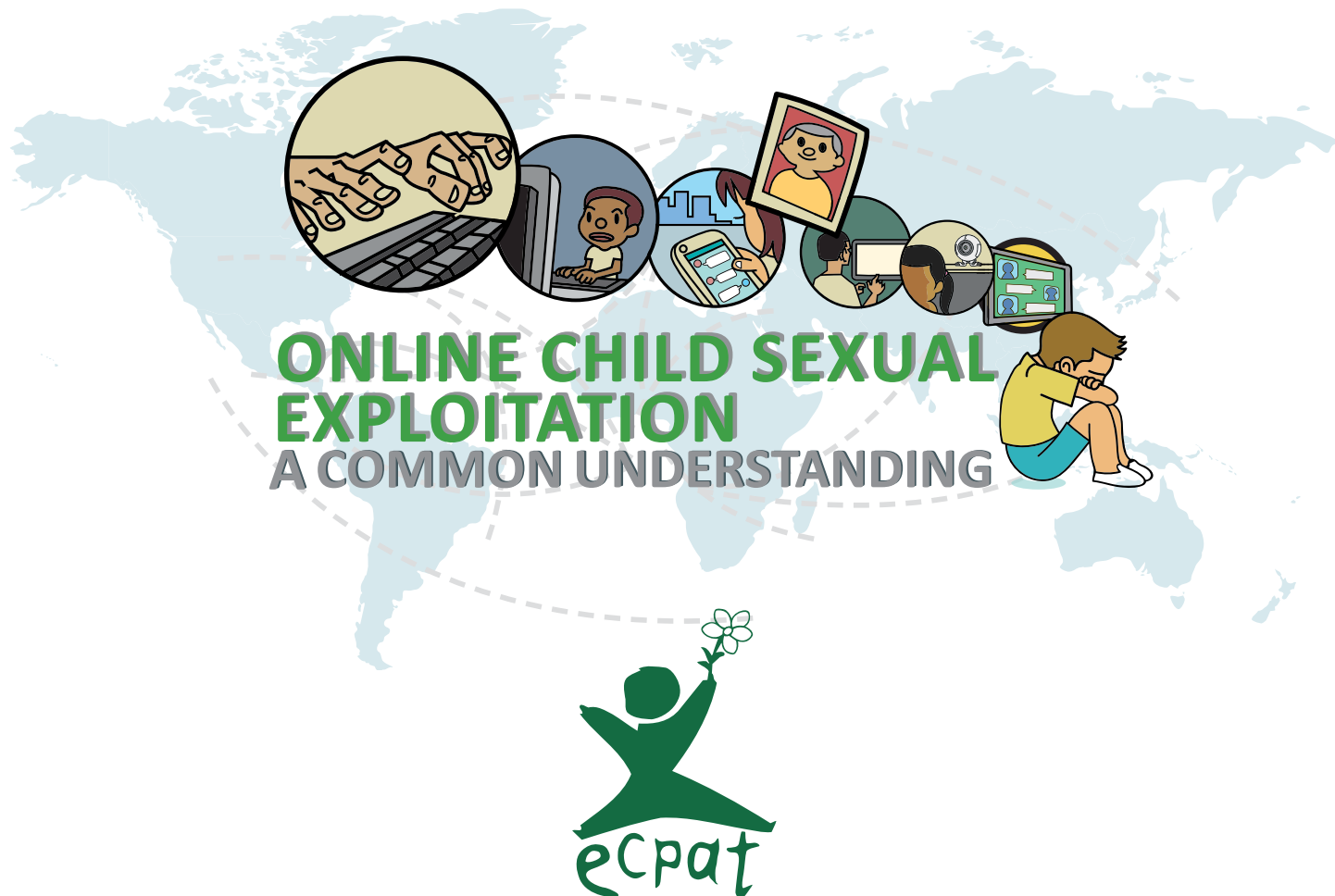
Email: info@ecpat.org

Website: www.ecpat.org

ISBN:

e-book: BN-60-146267

printed version: BN-60-146280



A user-friendly booklet on the manifestations, legal frameworks and technical terms and tools related to online child sexual exploitation

FOREWORD

Online child sexual exploitation is a global, fast-evolving problem which demands a comprehensive response. ECPAT works to increase the knowledge and to build the capacities of its members and other stakeholders in combating the issue of online child sexual exploitation. In order to be able to effectively work on a solution, the starting point is for all stakeholders to recognise what the problem is. This requires – at minimum – a baseline understanding of the various manifestations and on how offenders victimise children. Additionally, it is important to use a common language when discussing any approach to this problem, to ensure comprehension and prevent misperceptions about the nature and severity of this issue. Ideally, these shared notions should also be captured in national and regional legal frameworks criminalising and punishing such conducts with proportionate and dissuasive sanctions.

This booklet contains three series of factsheets related to online child sexual exploitation providing easy, ready-to-use resources to anyone interested in getting a better grasp of this issue. The first series is comprised of factsheets describing different manifestations of online child sexual exploitation. The second series covers the five relevant regional and/or international legal frameworks containing provisions regarding one or more of the manifestations of online child sexual exploitation. Finally, the third series consists of Internet and Technology factsheets describing terms and tools which are relevant to understand the Internet and how different technologies are (potentially) used by child sex offenders or those trying to obstruct the perpetrators.

Who is it for?

ECPAT aims to enable, empower and facilitate its members and other stakeholders in their efforts against online child sexual exploitation. The factsheets are available on www.ECPAT.org in various languages and can be used to support different activities such as awareness-raising or advocating with governments for stronger legal frameworks. These resources provide information in a concise and clear manner and can facilitate knowledge development amongst various stakeholders about the most pertinent issues related to online child sexual exploitation. Please use them for your work and reference.

ACRONYMS

| | |
|--------------|---|
| AU | African Union |
| CRC | Convention on the Rights of the Child |
| CoE | Council of Europe |
| CSAM | Child Sexual Abuse Material |
| CSEM | Child Sexual Exploitation Material |
| ECPAT | Ending the Sexual Exploitation of Children |
| ICMEC | International Centre for Missing and Exploited Children |
| ILO | International Labour Organisation |
| IP | Internet Protocol |
| ISP | Internet Service Provider |
| OPSC | Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography |
| OCSE | Online Child Sexual Exploitation |
| TOR | The Onion Router |
| URL | Uniform Resource Locator |

TABLE OF CONTENTS

| | |
|--|-----------|
| Foreword | 2 |
| Acronyms | 4 |
| Section 1: Manifestations | 6 |
| 1. Child Sexual Abuse/Exploitation Material | 7 |
| 2. Online Grooming for Sexual Purposes | 10 |
| 3. Sexting | 12 |
| 4. Sexual Extortion | 14 |
| 5. Live Online Child Sexual Abuse or Live Streaming of Child Sexual Abuse | 17 |
| Section 2: Legal | 20 |
| 1. The Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (OPSC) | 21 |
| 2. The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse | 24 |
| 3. The Council of Europe Convention on Cybercrime | 27 |
| 4. International Labour Organisation (ILO) Convention 182 concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour | 30 |
| 5. The African Union (AU) Convention on Cyber Security and Personal Data Protection | 33 |
| Section 3: Internet and Technology | 36 |
| 1. What is an IP-address? | 37 |
| 2. What is Filtering and Blocking? | 39 |
| 3. What is Encryption? | 41 |
| 4. What is TOR? | 43 |
| 5. What are Hashes? What is Photo DNA? | 45 |
| 6. What is Cloud Computing? | 48 |
| 7. What are Splash Pages? | 50 |

The background of the slide is a light blue world map. Overlaid on the map are several dashed white lines that represent global communication or data networks, connecting various continents and regions.

Section 1: MANIFESTATIONS

This section compiles factsheets covering five different manifestations of online child sexual exploitation including child sexual abuse material (CSAM) as well as digitally produced CSAM; Online grooming; Sexting; Sexual extortion and live online child sexual abuse. These factsheets follow the definitions as presented in the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse and describe the main characteristics of each manifestation.

1 Child Sexual Abuse/ Exploitation Material

DEFINITIONS

Child Sexual Abuse/Exploitation Material

Child sexual abuse material (CSAM), as the preferred term of choice to 'child pornography', refers to materials depicting acts of sexual abuse and/or focusing on the genitalia of the child.

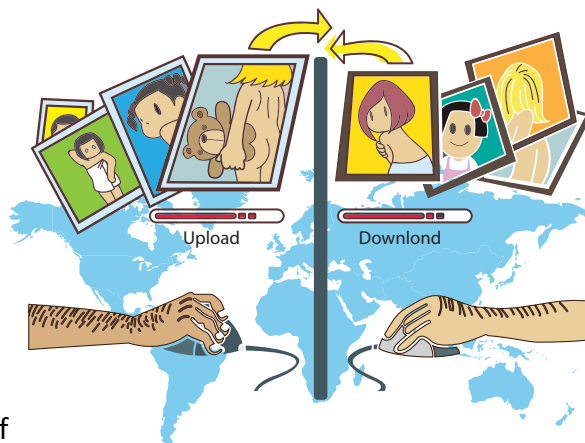
The term 'child sexual exploitation material' (CSEM) can be used in a broader sense to encompass all other sexualised material depicting children.

These materials include children of all ages, boys and girls, and differ in level of severity of the abuse and acts ranging from children posing sexually to gross assault.

Computer/Digitally Generated CSAM/CSEM

The term 'computer (or digitally) generated child sexual abuse material' encompasses all forms of material representing children involved in sexual activities and/or in a sexualised manner, with the particularity that the production of the material does not involve actual contact abuse of real children but is artificially created using digital tools to appear as if real children were depicted. It includes what is referred to as 'virtual child pornography'.

Although computer generated CSAM/CSEM does not involve harm to a real child, it is still dangerous because (i) it may be used in grooming children for sexual exploitation; (ii) it sustains a market for child sexual abuse material; and (iii) it enables a culture of tolerance for the sexualisation of children and cultivates demand.



This is (partly) criminalised by the following legal frameworks:

The Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (OPSC)

includes producing, distributing, disseminating, importing, exporting, selling or possessing 'child pornography' for the purpose of sexual exploitation of the child. Excludes accessing and mere possession of 'child pornography'. Definition of 'child pornography' is not inclusive of digitally/computer generated CSAM as defined in the Terminology Guidelines;

The Council of Europe Convention on Cybercrime (Budapest Convention)

includes producing, offering or making available, distributing or transmitting, procuring and possessing 'child pornography' through a computer system. Definition of 'child pornography' covers 'realistic images representing a minor engaged in sexually explicit conduct' and 'a person appearing to be a minor engaged in sexually explicit conduct';

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)

includes producing, offering or making available, distributing or transmitting, procuring, possessing and knowingly obtaining access to (computer generated) 'child pornography'. Definition of 'child pornography' is not inclusive of digitally/computer generated CSAM as defined in the Terminology Guidelines;

International Labour Organisation Convention 182 concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour (ILO Convention 182)

only covers the use, procuring or offering of a child for the production of 'pornography'. The Convention does not contain any definition of 'child pornography' or CSAM/CSEM;

The African Union Convention on Cyber Security and Personal Data Protection (AU Cyber Convention)

includes producing, registering, offering, manufacturing, making available, disseminating or transmitting, procuring, importing or exporting and possessing 'child pornography'. Definition of 'child pornography' is inclusive of digitally/computer generated CSAM as defined in the Terminology Guidelines.

Offenders and Modus Operandi

- Offenders are primarily motivated by their **sexual interest** in children or by **financial gain**;
- They operate **alone** or as part of a **network**;
- They use **different devices, software and/or the Internet** to produce, access or share materials;
- They sometimes apply **encryption methods** and may also use more **hidden online platforms** to conceal their conduct and avoid being detected¹;
- (Computer generated) CSAM/CSEM is sometimes used by offenders **to groom or manipulate children** into engaging in sexual activities.

Criminal Offenses

- Producing CSAM/CSEM;
- Obtaining access or procuring;
- (Mere) possessing;
- Offering or making available;
- Importing or exporting;
- Distributing, disseminating or transmitting;
- Registering;
- Selling.

What can you do?

- Advocate for stronger legal frameworks that criminalise all conducts related to CSAM/CSEM;
- Advocate for better resources for law enforcement, such as dedicated capacity and tools to tackle CSAM/CSEM and identify victims;
- Advocate and cooperate with the private sector, such as Internet Service Providers, to implement policies to disrupt circulation of CSAM/CSEM;
- Educate and raise awareness about CSAM/CSEM including online risks and online safety;
- Conduct research and collect relevant information to enhance understanding about the scope and characteristics of CSAM/CSEM;
- Report when you come across material online.

1. Please see ECPAT Factsheet: what is Encryption?

2 Online Grooming for Sexual Purposes

DEFINITION

Online Grooming for Sexual Purposes

Online grooming for sexual purposes is the process of establishing/building a relationship with a child through the use of the Internet or other digital technologies to facilitate either online or offline sexual contact with that person.

Acts of grooming are not limited to acts where a physical, in-person meeting has been attempted and/or occurred but also applies to acts conducted online.

Offenders and Modus Operandi

- Offenders are primarily motivated by their **sexual interest** in children or by **financial gain**;
- They operate **alone** or as part of a **network**;
- Offenders target victims by **assessing** their **vulnerability** (e.g. self-confidence, parental control) or by targeting children randomly;
- **Contact** with a child is generally initiated **online** (e.g. in chatrooms, gaming sites or social media platforms), but offline grooming also occurs;
- Grooming usually involves establishing an **emotional connection** with a child to gain the child's trust (also called long term grooming);
- Offenders can also focus on quickly gaining leverage over a victim rather than first establishing a trusting relationship;
- Groomers sometimes also **groom others** such as the child's peers, family and community-at-large; **Grooming behaviours** include filling the needs of a child by giving e.g. attention and gifts, psychological coercion, manipulation, 'sexually educating' and desensitising a child;



- Groomers progressively **sexualise the relationship** with the child (either quickly or slowly);
- Groomers commonly use **isolation, secrecy and blame** to sustain the child's participation and silence.

Legal Frameworks

- Grooming is criminalised in the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse;
- The **Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse** contains article 23 on the solicitation of children or the act of proposing a child to meet for the purpose of producing 'child pornography'. In addition, article 22 criminalises the corruption of children or the act of causing a child to witness sexual abuse or sexual activities;
- Additionally the **African Union Convention on Cyber Security and Personal Data Protection** criminalises the act of facilitating or providing access to pornographic material to a minor. Article 29(3)(1)(d) could capture elements of grooming.

What can you do?

- Advocate for stronger legal framework that criminalises the act of (online) grooming for sexual purposes;
- Advocate for better resources for law enforcement, such as dedicated capacity and tools to tackle the issue of online grooming;
- Advocate and cooperate with the private sector, such as Internet Service Providers, to implement measures to provide safe online environments for children;
- Educate and raise awareness about online grooming;
- Conduct research and collect relevant information to enhance understanding about the issue of online grooming;
- Report when you are aware of a situation where a child is targeted by groomers online;
- Provide support and care for victims.

3 Sexting

DEFINITION

Sexting

'Sexting', has been defined as the 'self-production of sexual images', or as 'the creating, sharing and forwarding of sexually suggestive nude or nearly nude images through mobile phones and/or the internet'.

It is a frequent practice among young persons and often a consensual activity between peers. There are also many forms of 'unwanted sexting'. This refers to the non-consensual aspects of the activity, such as sharing or receiving unwanted sexually explicit photos or messages.



Why and How do Children Engage in Sexting?

- Children themselves generally record and share images at their **own initiative or at the request** of another person;
- Images can be recorded with **different devices**. Often mobile phones are used to produce content that is shared via text, chat or social media platforms online;
- **Content is shared** with a boyfriend or girlfriend, other peers or people they are communicating with;
- Childrens' **motivation** for sexting can vary, including gratification in a sexual relationship, experimenting, soliciting compliments or attention and affirming a commitment to someone. Their motivation can also be related to **peer pressure**;
- Sexting is problematic as children often do not understand the **potential consequences** of their behavior and do not take measures to hide identifying information;
- Sexting is even more problematic when the content produced involves **criminal or abusive elements** such as adult involvement or lack of consent in sharing it;

- Sexting **makes children vulnerable** to becoming victims of sexual extortion,² (cyber)bullying and sometimes having their picture copied or used in collections of child sexual abuse/exploitation material.

Criminal Offense

Sexting is not criminalised in any of the relevant regional or international legal instrument on sexual exploitation of children. However, in some countries the law may consider sexting between children as violation of 'child pornography' laws because it involves production, offering and distribution of a sexual picture of a minor. The person recording and/or sending sexually explicit messages of a child, could be charged with production and distribution of child sexual abuse/exploitation material. In addition, the person receiving the material could be charged with possession of or accessing child sexual abuse/exploitation material.

In dealing with cases related to sexting, it is crucial to not blame children for self-generation of content that may have put them in an abusive/exploitative situation, or hold the child criminally liable for the production of child sexual abuse material. While many prosecutors and law enforcement will not prosecute children for engaging in sexting, in some jurisdictions children have in fact been charged with child sexual abuse/ exploitation material offenses.

What can you do?

- Educate and raise awareness among children, parents and caregivers about the risks and potential consequences of sexting;
- Advocate and cooperate with Internet Service Providers to prevent circulation of sexting content online and advocate with mobile operators to implement appropriate measures for collaboration with authorities when required (e.g. sharing user data on request).

2. Please see ECPAT OCSE Manifestations factsheet - Sexual extortion

4 Sexual Extortion

DEFINITION

Sexual Extortion

Sexual extortion, also called 'sextortion', is the blackmailing of a person with the help of (self-generated) images of that person in order to extort sexual favours, money, or other benefits from her/him under the threat of sharing the material beyond the consent of the depicted person (e.g. posting images on social media).

When carried out against children, sexual extortion involves a process whereby children or young people are coerced into continuing to produce sexual material and/or told to perform distressing acts under threat of exposure to others of the material. In some instances, the abuse spirals so out of control that victims have attempted to self-harm or commit suicide as the only way of escaping it.



Offenders and Characteristics of Sexual Extortion

- Perpetrators often rely on a position of authority or a **perceived imbalance of power** rather than on physical violence or force to coerce a child into sexual favours or money;
- The psychological coercion generally manifests with **threat of withholding certain benefits or threat of undesirable consequences** if demands are not met;

- The sexual component could involve a **perpetrator's demand** for any form of unwanted sexual activity, such as exposing private body parts, posing for sexual photographs, or submitting to sexual or physical abuse during a meeting offline;
- The sexual component can also be reflected in the **methods applied to obtain goods, services or money**. For example perpetrators gain access to self-generated sexual content³ or compromising images of a victim and use this material to blackmail for money;
- Sexual extortion can involve the (threat of) dissemination of compromising images online or to peers. This in turn can result in **other negative consequences** like (cyber)bullying which further victimises or harms the child.



What can you do?

- Advocate for stronger legal frameworks that specifically criminalise sexual extortion;
- Advocate for better resources for law enforcement to tackle the issue of sexual extortion;
- Advocate and cooperate with Internet Service Providers to prevent circulation of child sexual abuse/exploitation content online, in order to limit sexual extortion opportunities for perpetrators;
- Educate and raise awareness among children, parents and caregivers about the risks and potential consequences of sexting;
- Report when you come across sexting or child sexual abuse/ exploitation material online.

3. Please see ECPAT OCSE Manifestations factsheet – Sexting

Criminal Offense

Sexual extortion is not explicitly criminalised in any of the relevant regional or international legal instruments on sexual exploitation of children.

However, article 34(c) of the Convention on the Rights of the Child criminalises 'the exploitative use of children in pornographic performances and materials' and article 21(1)(a-b) of **the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse** criminalises the act of causing and coercing children to engage in 'child pornographic performances'. The same accounts for the act of soliciting children to produce 'child pornography' which is criminalised in article 23. The act of engaging in sexual activities with a child is criminalised, where coercion, force or threats are present; when this person abuses a recognised position of trust, authority or influence over the child; or a particularly vulnerable situation of the child. These articles could be interpreted to capture elements of sexual extortion.

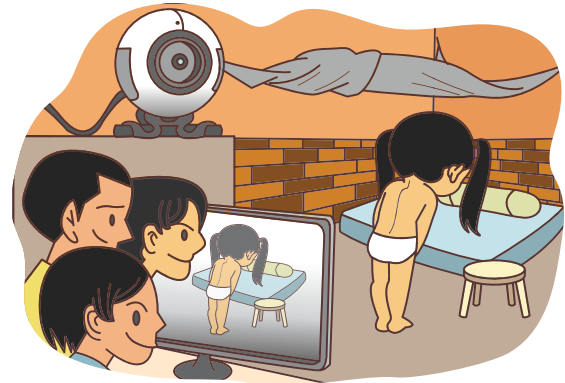
In addition, the conventions that do criminalise the production, procuring, distribution or offering of child sexual abuse/ exploitation material - i.e. **the Council of Europe Convention on Cybercrime; the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse; the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (OPSC) and the African Union Convention on Cyber Security and Personal Data Protection** - contain language that might capture elements of sexual extortion.

5 Live Online Child Sexual Abuse or Live Streaming of Child Sexual Abuse

DEFINITION

Live Online Child Sexual Abuse

Live online child sexual abuse involves coercion of a child to participate in sexual activities, alone or with other persons. The sexual activity is, at the same time, transmitted live or 'streamed' over the Internet and watched by others remotely. Often, the persons watching remotely are the persons who have requested and/or ordered the sexual abuse of the child, dictating how the act should be carried out, and those persons may be paying for the abuse to take place.



Offenders and Modus Operandi

- Offenders watching live sexual abuse of children via e.g. webcam may gain access through **intermediaries or facilitators**;
- Facilitators are sometimes the child's **family** or **community members** who force the child to perform in front of a webcam and communicate with and elicit (potential) customers;
- The offender and the facilitator or child **agree** on a **time and date** when the abuse will take place and the offender will log on. These appointments are made via chat, e-mail, phone and any other available channel;
- Additionally the parties involved will **agree** on a **price** the offender will pay, usually through common legitimate payment services. The amounts paid are generally small to prevent raising suspicion related to the transactions;

- Different platforms such as Skype or webcam-supported chat sites are being used to **live stream** the abuse over the Internet. This allows offenders to **view** the abuse in real time and/or to **direct** it through the chat or voice function;
- In some communities, there can be a level of **social tolerance** permitting the crime. This is related to several factors such as poverty and a limited understanding of the Internet, the implications for the child - particularly when there is no physical sexual abuse involved - or the illegality of these acts. Live online child sexual abuse can be perceived as an easy and quick source of income.

Criminal Offense

Live online child sexual abuse is not explicitly criminalised in any of the relevant regional or international legal frameworks on sexual exploitation of children.

However, article 21(1)(a-b) of the **Lanzarote Convention** criminalises the act of causing and coercing children to engage in ‘child pornographic performances’ as well as knowingly attending ‘child pornographic performances’ (c). Moreover article 24 criminalises the act of aiding or abetting these actions which could be applied to people facilitating or encouraging the offense. such is also the case of the Convention on the Rights of the Child in its article 34(c) and of the ILO Convention 182 in its article 3 (b).

The **Optional Protocol to the Convention on the Rights of the Child on the Sale of Children Child Prostitution and Child Pornography (OPSC)** article 3(1)(a) criminalises the act of offering, delivering or accepting by whatever means, a child for the purpose of sexual exploitation.

Similarly the **International Labour Organisation Convention 182 concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour** article 3(b) criminalises the use, procuring or offering of a child for [...] pornographic performances.

These articles could be interpreted to capture acts related to live online child sexual abuse by both offenders and facilitators.

Since live online child sexual abuse involves the act of live streaming of child sexual activities rather than actually recording a picture or video depicting child sexual abuse, it can be difficult to obtain evidence of the abuse and charge offenders for possession, production or dissemination of child sexual abuse/exploitation material.



What can you do?

- Raise awareness and sensitise communities at large about the illegality, impact and risks related to live online/streaming of child sexual abuse;
- Advocate for stronger legal frameworks that specifically criminalise live online/streaming of child sexual abuse or 'child pornographic performances';
- Advocate for better resources for law enforcement to tackle this issue;
- Advocate with financial institutions to trace and follow-up on suspicious transactions that could be related to the crime.

Section 2:

LEGAL

The legal factsheets discuss five relevant regional and/or international legal instruments containing provisions regarding one or more of the manifestations of online child sexual exploitation. These include the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography; the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse; the Council of Europe Convention on Cybercrime; the International Labour Organisation Convention 182 concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour; and the African Union Convention on Cyber Security and Personal Data Protection. The factsheets contain information on how child sexual abuse material – often legally referred to as "child pornography" – is defined in the instruments and what manifestations of online child sexual exploitation are or can be addressed through the legal articles. The strengths and weaknesses of each Convention are also highlighted.

NB: please note that for the legal factsheets we will use the term 'child pornography' rather than the preferred term 'child sexual abuse/exploitation material' because this is the language which is used in all of the Conventions.

Since the Conventions do not contain a specific definition for computer or digitally generated child sexual abuse material, we will refer to it following the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse.

1 The Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (OPSC)

To help stem the growing abuse and exploitation of children worldwide, the United Nations General Assembly in 2000 adopted the Optional Protocol to the Convention on the Rights of the Child to prevent the sale of children, child prostitution and child pornography (OPSC).

OPSC and Online Child Sexual Exploitation

Concerning online child sexual exploitation, the OPSC implies obligations for State Parties to criminalise and punish, by appropriate penalties, activities related to (among others):

Article 3:

- (1)(i)(a) Offering, delivering or accepting by whatever means, a child for the purpose of sexual exploitation of the child;
- (1)(ii)(c) Producing, distributing, disseminating, importing, exporting, selling or possessing child pornography for the purpose of sexual exploitation of the child;
- (2) Attempting to commit any of these acts and to comply or participate in any of these acts.

Definition of 'child pornography'

Article 2 (c):

“any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes”

What is an optional protocol?

An optional protocol is a stand-alone treaty that is open to signature, accession or ratification by countries who are party to the main existing treaty it complements and adds to. Usually, it provides for procedures or addresses a substantive area related to the treaty. They are optional because States must independently choose whether or not to be bound by them.



STRENGTHS OF THE OPTIONAL PROTOCOL (OPSC)

- ✓ The optional protocol promotes a holistic approach addressing underlying causes such as poverty; this approach includes e.g. prevention, awareness-raising and reporting obligations;
- ✓ It contains provisions concerning jurisdiction, extradition and mutual assistance to further facilitate and enhance international cooperation;
- ✓ It criminalises those attempting, complying or participating in the conduct, which can be used to prosecute offenders and facilitators;
- ✓ It calls for measures to protect the rights and interests of child victims at all stages of the criminal justice process.

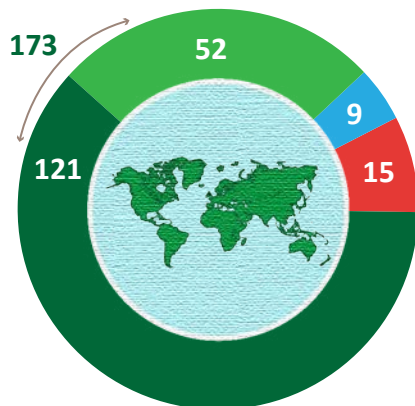
WEAKNESSES OF THE OPTIONAL PROTOCOL (OPSC)

It does not specifically define and criminalise all the conducts related to online child sexual exploitation, namely:

- ✗ Knowingly accessing or viewing 'child pornography';
- ✗ Merely possessing 'child pornography';
- ✗ Digitally generated child sexual abuse material;
- ✗ Online grooming for sexual purposes;
- ✗ Sexual extortion;
- ✗ Live online child sexual abuse.

Why should your Country become a State Party to the OPSC?

- It complements the Convention on the Rights of the Child and extends the measures to protect children from 'child pornography';
- It promotes international cooperation.



To date, the OPSC has been ratified by 173 Member States of whom 121 signed and ratified it and 52 acceded to the Protocol. 9 States have signed but not ratified it and 15 States have not yet signed nor ratified it.

2 The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse

In 2007, the Council of Europe (CoE) adopted the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, also known as 'the Lanzarote Convention'. Any State around the world can become a party to the Convention. Its objectives are: to prevent and combat sexual exploitation and sexual abuse of children (a), to protect the rights of child victims (b) and to promote national and international co-operation (c).

The Lanzarote Convention and Online Child Sexual Exploitation

The Lanzarote Convention imposes obligations to criminalise and punish with effective, proportionate and dissuasive sanctions (article. 27):

Article 20 (1) CHILD PORNOGRAPHY

- a. producing;
- b. offering or making available;
- c. distributing or transmitting;
- d. procuring;
- e. possessing;
- f. knowingly obtaining access.

Definition of 'child pornography'

Article. 20 (2):

“any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child’s sexual organs for primarily sexual purposes”

Article 21 (1) CHILD PORNOGRAPHIC PERFORMANCES

- a. recruiting children/causing;
- b. coercing/exploiting children;
- c. knowingly attending.

Article 22 CORRUPTION OF CHILDREN

Causing a child to witness sexual abuse or sexual activities.

Article 23 SOLICITATION OF CHILDREN

Intentionally proposing by an adult, through information and communication technologies to meet a child who has not reached the minimum age for sexual activities/consent, for engaging in sexual activities with a child or producing child pornography, followed by material acts leading to such a meeting.

In 2015, the Lanzarote Committee published an opinion inviting Member States to criminalise also cases where the unlawful sexual activities are committed exclusively online.

Article 24 AIDING, ABETTING, ATTEMPT

Facilitating/encouraging offense.

How is the Convention monitored?

The Lanzarote Committee was established to monitor whether State Parties effectively implement the Lanzarote Convention. The aim is to create a comparative overview of the situation, as well as to foster the exchange of good practices and encourage the detection of difficulties. The Committee is also mandated to facilitate the collection, analysis and exchange of information between states to improve their capacity to prevent and combat child sexual exploitation.



Why should your country become a State Party to the Lanzarote Convention?

- It is the most advanced and complete legally binding international instrument on child sexual exploitation;
- It criminalises sexual exploitation in a very comprehensive manner;
- It would help prevent exploitation of children at home and abroad;
- It promotes international cooperation in sharing information, investigating and prosecuting offenders.

STRENGTHS OF THE CONVENTION

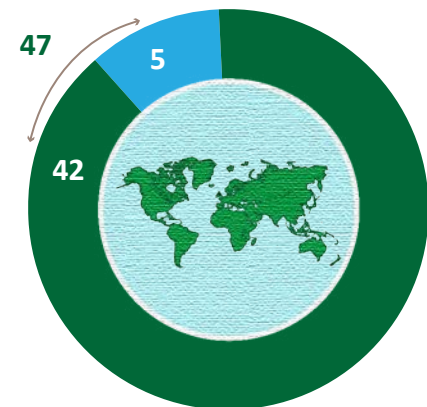
- ✓ It criminalises all relevant conduct in relation to 'child pornography';
- ✓ It criminalises the act of causing or coercing children to engage in 'child pornographic performances' Which captures live online child sexual abuse and elements of sexual extortion;
- ✓ It criminalises the act of engaging in sexual activities with a child, where use is made of coercion, force or threats, or when this person abuses a recognised position of trust, authority or influence over the child or a particularly vulnerable situation of the child. This could capture elements of sexual extortion;
- ✓ It criminalises the act of exposing a child to sexual activities or abuse as well as solicitation of children, which captures aspects of online grooming;
- ✓ It criminalises those assisting or aiding and abetting sexual exploitation.

WEAKNESSES OF THE CONVENTION

It does not specifically define or criminalise all forms of online child sexual exploitation, including:

- ✗ Sexual extortion
- ✗ Digitally generated child sexual abuse material

Parties have the right to not criminalise digitally generated child sexual abuse material conform article 20(1)(3)



To date, the Lanzarote Convention has been signed by all 47 Council of Europe Member States. 42 of these States have both signed and ratified it, and 5 States signed without ratifying the Convention.

3 The Council of Europe Convention on Cybercrime

The Convention on Cybercrime, also known as the 'Budapest Convention', is the first international treaty seeking to address Internet and computer crime. It pursues a common criminal policy to facilitate detection, investigation and prosecution of conducts directed against or misusing the confidentiality, integrity and availability of computer systems, networks and computer data. This policy includes adopting and harmonising domestic criminal and procedural law as well as fostering international cooperation. The Convention was opened for signature on 23 November 2001 and entered into force on 1 July 2004.

Budapest Convention and Online Child Sexual Exploitation

Concerning online child sexual exploitation, the Budapest Convention imposes obligations to criminalise and punish with effective, proportionate and dissuasive sanctions (article 13), any conduct involving:

Article 9 (1) CHILD PORNOGRAPHY

- Producing child pornography for the purpose of its distribution through a computer system;
- Offering or making available child pornography through a computer system;
- Distributing or transmitting child pornography through a computer system;

Definition of 'child pornography'

Article 9 (2):

“material that visually depicts a minor engaged in sexually explicit conduct (a); a person appearing to be a minor engaged in sexually explicit conduct (b); realistic images representing a minor engaged in sexually explicit conduct (c)”

- Procuring child pornography through a computer system for oneself or another person;
- Possessing child pornography in a computer system or on a computer-data storage medium.

STRENGTHS OF THE CONVENTION

- ✓ It uses clear definitions;
- ✓ It criminalises all the relevant conducts in relation to 'child pornography', including 'procuring';
- ✓ It criminalises those aiding or abetting the commission of the offences, which can be used to prosecute facilitators;
- ✓ It acknowledges the need to pursue a common criminal policy and sets out procedural law in relation to e.g. intercepting and seizing data to be established for the purpose of investigation and offender identification;
- ✓ It contains provisions concerning mutual assistance as well as extradition rules to further facilitate and enhance international cooperation.

WEAKNESSES OF THE CONVENTION

It does not specifically define and criminalise all the conducts related to online child sexual exploitation:

- ✗ Mere production of 'child pornography';
- ✗ Online grooming;
- ✗ Sexual extortion;
- ✗ Live online child sexual abuse;

States are not obligated to criminalise:

- ✗ Procurement or possession of 'child pornography';
- ✗ Digitally generated child sexual abuse material.

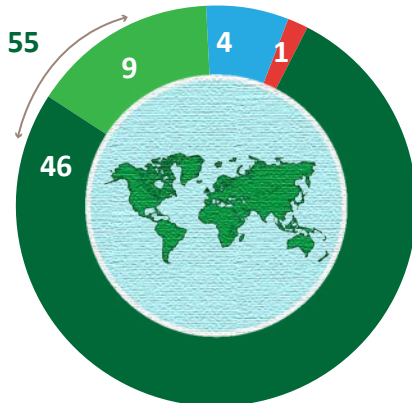
Law enforcement interests vs. human rights

In its preamble the Convention emphasises the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights, specifically the right to hold opinions without interference; freedom of expression; and the rights concerning the respect for privacy. It is mindful of the right to protection of personal data.



Why should your country become a State Party to the Budapest Convention?

- It is the first international treaty seeking to address Internet and computer crime and it addresses the issue of 'child pornography' as a cybercrime issue providing clear provisions for data gathering online;
- It promotes international cooperation;
- It promotes cooperation between State Parties and industry.



To date, the Budapest Convention has been ratified by 55 States. 46 of them have both signed and ratified it and 9 States acceded to the Convention. 4 States have signed but not ratified it and 1 Member States of the Council of Europe have not signed nor ratified it.

4 International Labour Organisation (ILO) Convention 182 Concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour



In 1999, the International Labour Organisation (ILO) adopted the Convention No. 182. By ratifying this Convention, a country commits itself to taking immediate action to prohibit and eliminate and protect children under 18 from the worst forms of child labour. The necessary actions range from a reform of laws and their enforcement, to practical and direct help to children and families.

ILO Convention and Online Child Sexual Exploitation

The Convention calls on Members to take immediate and effective measures to secure the prohibition and elimination of 'the worst forms of child labour' and to ensure effective implementation of its provisions, including penal and other sanctions.

For the purposes of this Convention, and in relation to the issue of sexual exploitation of children, this comprises:

Article 3:

- (b) The use, procuring or offering of a child for prostitution, for the production of pornography or for pornographic performances;
- (d) Work which, by its nature or the circumstances in which it is carried out, is likely to harm the health, safety or morals of children.

Worst Forms of Child Labour Recommendation (No. 190)

The Worst Forms of Child Labour Recommendation (No. 190) was adopted by the ILO in 1999. The provisions of this Recommendation supplement those of Convention No. 182, and should be applied in conjunction with them. It calls e.g. for ratifying countries to 1) enhance international cooperation 2) ensure that the pre-defined worst forms of child labour are criminalised and 3) provide for measures to ensure effective enforcement of provisions.

STRENGTHS OF THE ILO CONVENTION 182

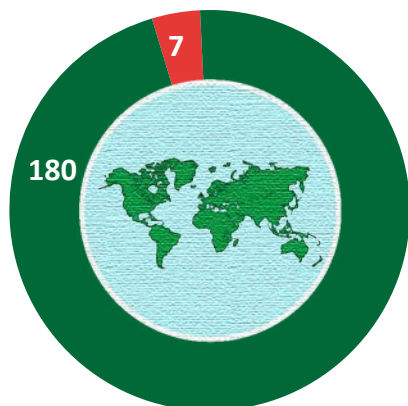
- ✓ It criminalises 'child pornographic performances', which captures conduct related to live online sexual abuse;
- ✓ It promotes a holistic approach including e.g. the rehabilitation and social integration of victims;
- ✓ The ILO Monitoring Body can issue recommendations to the States who have ratified the Convention. If the State does not comply with these recommendations, the ILO can take the case up to the International Court of Justice. This implies a considerable authority to ensure implementation of its provisions.

WEAKNESSES OF THE ILO CONVENTION 182

- ✗ The ILO Convention focuses on labour and therefore does not cover all the online sexual exploitation conducts (e.g. sexual extortion, online grooming);
- ✗ It emphasises national sovereignty over international law which might lessen States obligation to act;
- ✗ There are no minimum thresholds States should comply with or meet with respect to national constitutions and legal frameworks;
- ✗ 'Child pornography' or child sexual abuse/exploitation material is not defined.

Why should your country become a State Party to the ILO Convention 182?

- It consolidates the global consensus against the worst forms of child labour;
- It calls for criminalising 'child pornography/ performances' as one of the worst forms of child labour, thereby complementing the child rights violation approach and providing an additional angle for prosecution;
- It promotes international cooperation which is relevant considering that the manifestations of child sexual exploitation as defined under Article 3(b) are borderless by nature of the Internet that is used by offenders to facilitate it.



To date, 180 out of 187 ILO Member States have ratified the Convention.

5 The African Union (AU) Convention on Cyber Security and Personal Data Protection



In June 2014, the African Union adopted the Convention on Cyber Security and Personal Data Protection. The goal of this Convention is to address the need for harmonised legislation in the area of cyber security in Member States of the African Union – including criminal procedural law - and to establish in each State Party a mechanism capable of combating violations of privacy. It calls for the establishment of an normative framework consistent with the African legal, cultural, economic and social environment. With respect to online child sexual exploitation the Convention specifically includes 'child pornography'.

The AU Convention and Online Child Sexual Exploitation

The Convention on Cyber Security and Personal Data Protection obligates States to take the necessary legislative and/or regulatory measures to make it a criminal offence to:

Article 29 (3) (1) CHILD PORNOGRAPHY

- (a) Produce, register, offer, manufacture, make available, disseminate and transmit;
- (b) Procure for oneself or for another person, import or have imported, and export or have exported;
- (c) Possess an image or representation of child pornography in a computer system or on a computer data storage medium;
- (d) Facilitate or provide access to images, documents, sound or representation of a pornographic nature to a minor.

Definition of 'child pornography'

Article 1:

"any visual depiction, of sexually explicit conduct, where:

- (a) the production of such visual depiction involves a minor;*
- (b) such depiction involves a minor engaging in sexually explicit conduct or when images of their sexual organs are produced or used for primarily sexual purposes and exploited with or without the child's knowledge;*
- (c) such visual depiction has been created, adapted, or modified to appear that a minor is engaging in sexually explicit conduct."*

Why should your country become a State Party to the AU Convention?

- This Convention lays a progressive foundation that can encourage your State to enhance the approach to child pornography.

Caution needs to be taken to ensure protection of privacy and criminalisation of the other manifestations of online child sexual exploitation.

STRENGTHS OF THE CONVENTION

- ✓ It criminalises all relevant conducts in relation to 'child pornography';
- ✓ It criminalises digitally generated child sexual abuse material;
- ✓ It criminalises the act of facilitating or providing access to pornographic content to a minor, which captures aspects of online grooming and sexual extortion;
- ✓ It outlines principles that ought to be adhered to in processing personal data to protect privacy (e.g. transparency, and security of personal data);
- ✓ It calls on mobilisation of all public and private actors, thereby promoting a holistic approach.

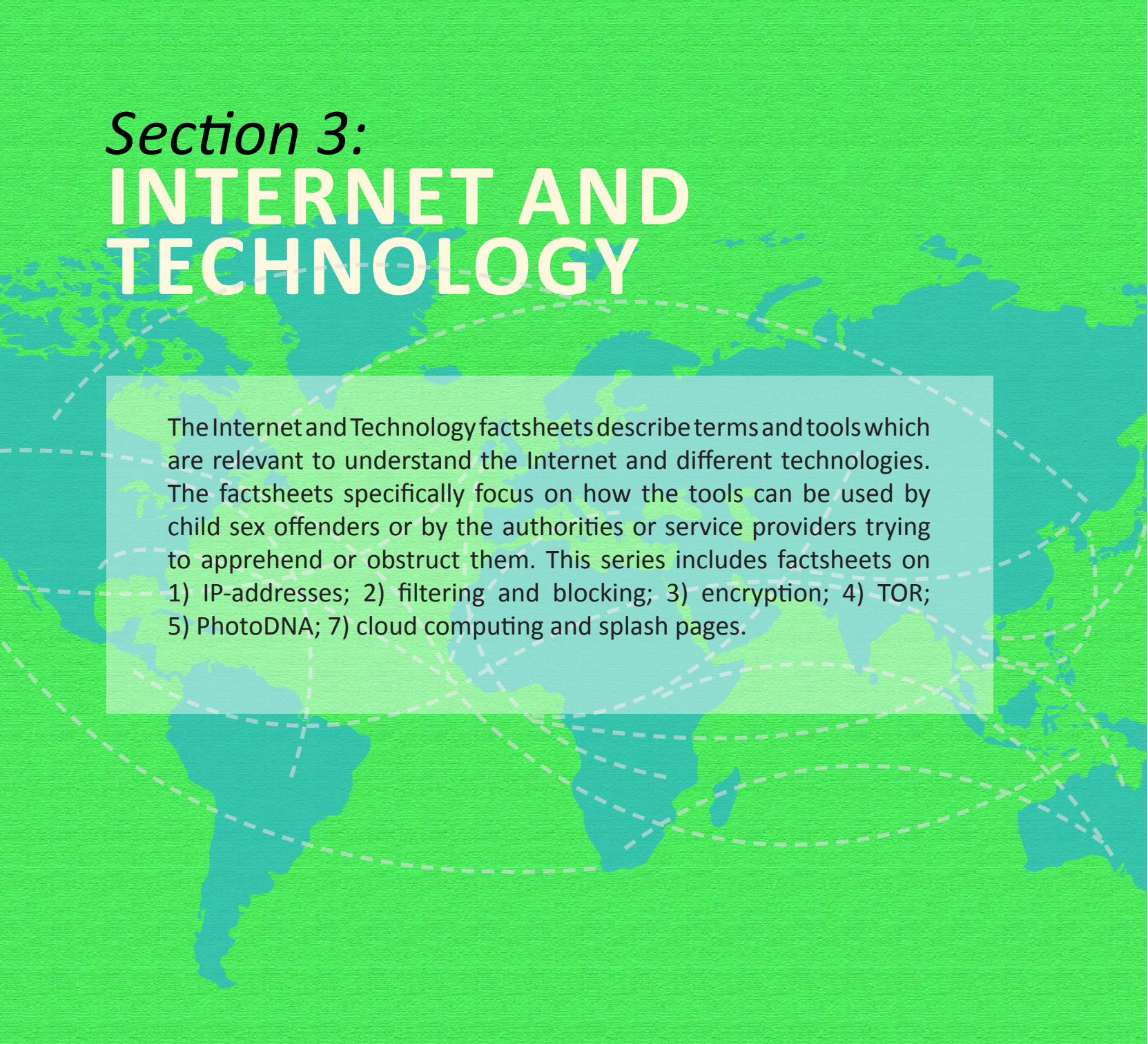
WEAKNESSES OF THE CONVENTION

The Convention does not define and criminalise all the conducts related to online child sexual exploitation:

- ✗ Online grooming;
- ✗ Sexual extortion;
- ✗ Live online child sexual abuse;
- ✗ It uses vague definitions that could be used to limit the freedom of speech;
- ✗ It does not specify clear minimum thresholds that national constitutions, legal frameworks and laws should meet and comply with.



8 states have signed the Convention not followed by ratification yet



Section 3: **INTERNET AND TECHNOLOGY**

The Internet and Technology factsheets describe terms and tools which are relevant to understand the Internet and different technologies. The factsheets specifically focus on how the tools can be used by child sex offenders or by the authorities or service providers trying to apprehend or obstruct them. This series includes factsheets on 1) IP-addresses; 2) filtering and blocking; 3) encryption; 4) TOR; 5) PhotoDNA; 7) cloud computing and splash pages.

1 What is an IP-address?

And how is it used for the identification of child sex offenders online

How Does it Work?

An IP-address is the identifier or unique signature of a device, which allows the device to be identified, pinpointed and differentiated from other devices that are connected to the Internet. Every device comes with its own IP-address whether it is a computer, television, gaming console or other device.

IP-addresses allow for communication between devices. In the same way that a person needs a post address to be able to send a letter, a remote computer needs the IP-address of a device to be able to communicate with it. IP-addresses thus enable users to send and retrieve data and ensure that communication and data reach the correct destination. It reveals information such as where the device is located and which Internet Service Provider is servicing it. This protocol is universal and works the same for every device or location.

FACTS



IP stands for Internet Protocol.

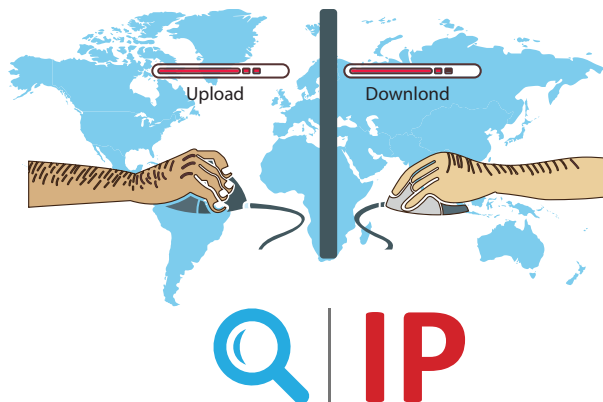
It is a technical language that allows two devices to communicate with each other over the Internet.

IP addresses can either be 'static' [never changing] or 'dynamic' [temporary].



IP-Address format

An IP-address consists of a set of numbers and dots. The number of available IP addresses is beginning to expand as a new version of the IP protocol - IP version 6 or IPv6 - becomes more widely used.



The Use of IP-addresses for Identification of Child Sex Offenders

When child sex offenders connect to the Internet, they use devices which have IP-addresses. These IP-addresses leave a trail of Internet activity. This can provide the authorities with an opportunity to track down the device and often will enable them to tell when and where the device was used. This in turn means the individual who was using the device to commit a crime may be identified.

The authorities can also request as per the local legislation in place Internet Service Providers (ISPs) to access (temporary) IP-address logs and activities on their servers for the purpose of user identification.

Unfortunately, offenders can take measures to hide their IP-address. One method is by using proxy servers. Rather than accessing a website directly, the user's request will be redirected through the proxy server that does not record the IP address of the device making the request. This offers a degree of anonymity. Another example is the use of IP-spoofers to mask the real IP-address and wrongfully present a different IP-address as the source of illegal conduct.

There are also other tools and Internet services available which can make finding an individual's IP address very difficult and time-consuming.

2 What is Filtering and Blocking?

And how is it used for child sexual abuse material

How Does it Work?

Many Internet Service Providers (ISPs) and other online service providers are keen to prevent their users from accessing web addresses that are known to contain child sexual abuse material. Additionally, they might want to prevent their users from uploading, exchanging or storing child sexual abuse images or videos using their platforms and services. To do this, they use filtering and blocking technologies.

Web addresses that are known to contain child sexual abuse material are placed on a list that is circulated directly to companies who might incorporate this list into a security policy for their service. Any attempt to reach an address on that list will be filtered out or blocked. The lists are compiled and provided by bodies such as hotlines and police agencies (e.g. INTERPOL). Filtering and blocking can also be applied for specific search terms or key words that are related to child sexual abuse (material).

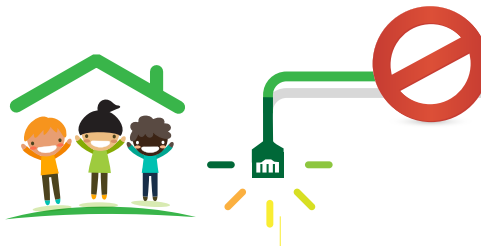
FACTS



The goal of filtering and blocking is to limit the availability of particular content online.

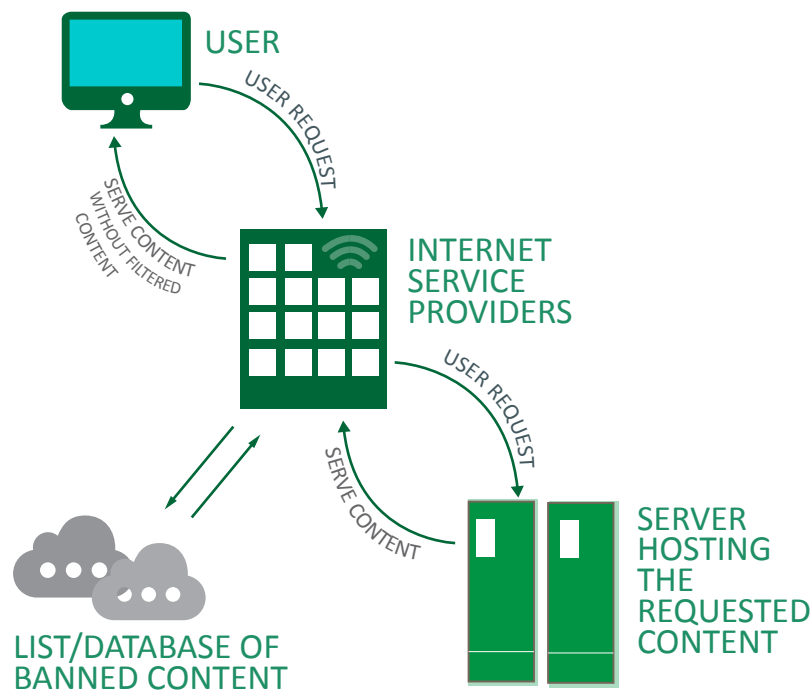
Filtering and blocking only impacts the material on the part of the Internet indexed by search engines.

Filtering and blocking can be based on: key words (e.g. search terms); banned URLs (e.g. websites); and hashes.



In a number of countries it is a legal requirement for ISPs to block child sexual abuse material.

Where an individual image is already known to the police, hashing technologies such as PhotoDNA, can be used to create a hash⁴ or digital fingerprint of an image. These hashes are then placed in a database and systems can subsequently identify any copies of that image that a user might attempt to upload, download, exchange or store on their service.



CAUTION

Filters cannot always distinguish between a match that refers to illegal content and those that do not. This creates the risk of content being wrongfully blocked (over-blocking).

Filtering and Blocking Child Sexual Abuse Material

The net effect and intention behind filtering and blocking technologies is to reduce or limit the availability of child sexual abuse material online. It contributes to a safer Internet by preventing unwanted exposure to this type of illegal content. Moreover it obstructs offenders attempting to access and share child sexual abuse material.

Filtering and blocking also has an important benefit to the victims depicted in the images. By making the images inaccessible, filtering and blocking mechanisms protect victims' privacy and reduce the possibility of further harm being inflicted on the child.

4. See factsheet - What are hashes? What is PhotoDNA?

3 What is Encryption?

And how is it used by child sex offenders online

How Does it Work?

Encryption is a means of disguising or hiding a message by applying a series of computer programmed steps [encryption software] so that should the message fall into 'the wrong hands' the person seeing or reading it will not be able to understand what it says. For example, it changes a message such as "I will meet you on Monday" to a coded message such as "p98hUls#yeb!"

This incomprehensible coded message - a ciphertext - is then sent over the Internet to a receiver. The person receiving the message must have a 'decoding key' (e.g. a password) that is unknown to others and provided to him by the sender to unlock or recover the original message. This process is called decryption. Without that key the message is unreadable or the image is unviewable.

FACTS



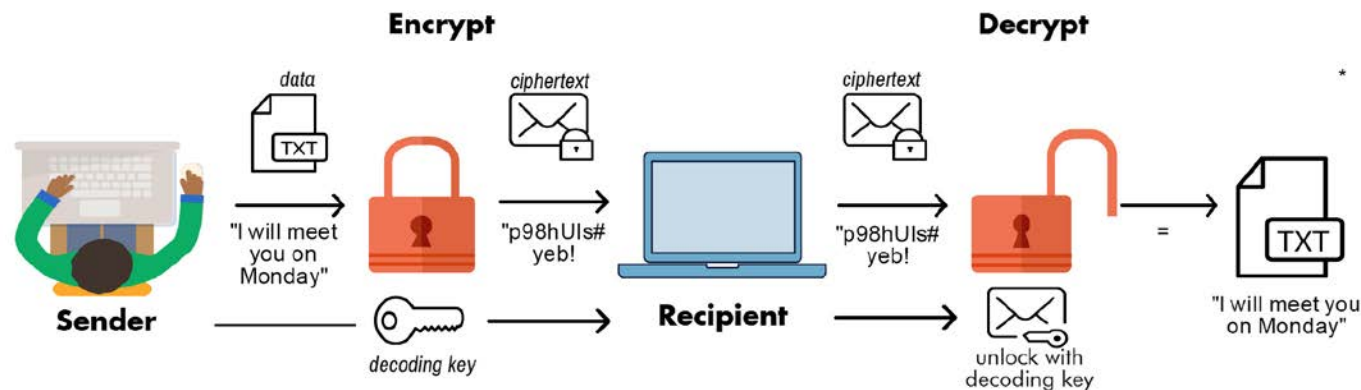
Encryption is applied to data sent from devices across many networks.

Encryption conceals data that is stored or transmitted.

Encryption is used to secure: data (e.g. files, pictures, computers), Internet transactions (e.g. banking), passwords, networks and E-mail.



The encryption/decryption process is as follows⁵:



Encryption Applied by Child Sex Offenders Online

Child sex offenders communicate with each other online using a variety of tools to conceal their identity and conduct from the authorities.

For example, perpetrators encrypt child sexual abuse material so it is not recognisable as such when apprehended by non-authorised persons or entities. Or they might encrypt computers or disks to prevent authorities from accessing or recognising incriminating evidence during a house search. Additionally, encryption allows offenders to verify the identity of those they are communicating with online.

Some weak encryption programmes can be broken by powerful computers but, for practical purposes, generally many of the strong encryption programmes that are widely available cannot be cracked without the decoding key.

Encryption contributes to additional complexity in law enforcement investigations.

5. Please note that this is one example and that there are different ways to encrypt and decrypt data

4 What is TOR?

TOR is **free software** for enabling anonymous communication. The name is derived from an acronym for the original software project name 'The Onion Router'.

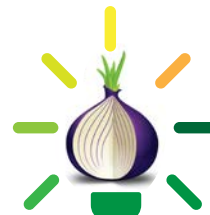
How Does it Work?

TOR diverts online traffic through a network in a way that conceals a user's location or identity. Instead of transporting traffic such as visits to websites or instant messages through a fixed predictable route [from user 'Kim' to the Website], TOR goes through a dynamically assigned route that becomes untraceable.

The TOR connection is encrypted. An unencrypted link is exposed to surveillance, allowing someone to learn what websites you visit by tracing back your IP-address.⁶ However, TOR uses an encrypted connection which means that at any point on the route from the origin Internet user to the destined location, it is not clear where the data is coming from or where it is going.

⁶ An IP-address reflects the identity of the user of a device [see factsheet: What is an IP-address?]

FACTS



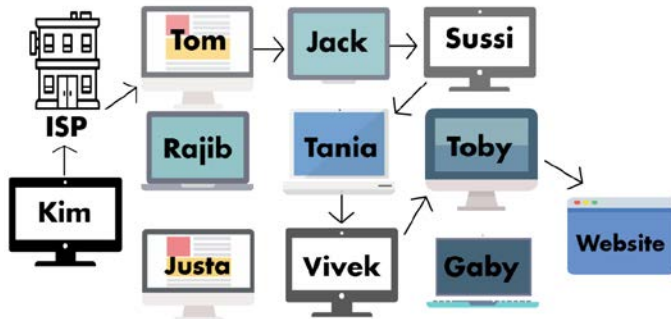
TOR is short for The Onion Router.

TOR software was developed by the US Naval Research Laboratory to protect US intelligence communication.

TOR has legitimate uses for users who want to maintain privacy; circumvent censorship; or protect themselves from repressive regimes or targeted monitoring.

TOR aims to conceal user identities and their online activity from surveillance and traffic analysis.





When Kim visits a website via the TOR network her traffic takes a random path through other people's computers to get to the website. At each intermediate point the source and destination information is stripped to make identification of the user extremely difficult. As a result, Internet Service Providers cannot track who she is and what sites she is visiting. Or TOR misleadingly presents the last exit node [Toby] as the communication source.

TOR Used by Child Sex Offenders Online

Child sex offenders use TOR to share child sexual abuse images or other content that facilitates and perpetuates a culture of child sexual abuse. Moreover, TOR allows them to connect with potential victims anonymously. Also TOR's hidden services allow for perpetrators to communicate secretly amongst each other. By using TOR, offenders avoid revealing their location or identity, thereby evading detection by Internet Service Providers (ISPs) and law enforcement. This way TOR complicates victim and offender identification.

TOR is the most popular software program used to access the parts of the Internet which are deliberately constructed to provide users with a level of anonymity or privacy. These anonymous websites and encrypted networks are referred to as the Darknet and are commonly accessed via TOR. It is believed that the most extreme child sexual abuse material is shared via TOR.

5 What are Hashes? What is PhotoDNA?

And their application to child sexual abuse material

How Does it Work?



⁷ Photo-DNA starts with an image that has been identified as child sexual abuse material by trusted sources, such as the National Centre of Missing and Exploited Children or law enforcement authorities.



PhotoDNA transforms (or 'hashes') the image into a black-and-white format and uniform size. It then divides the image into squares and assigns a numerical value that represents the unique shading found within each square. Together these numerical values compose the hash for that image.



Hash values of known images can be compared to other images to identify copies. This process is called the matching process and can be used to: 1) identify and flag harmful content online and 2) filter out known materials from collections of images.



The hash represents a unique digital identifier or signature for each image. Even if the image has been altered - e.g. when the image is re-sized or when colors are altered - the hash code remains the same for that image.

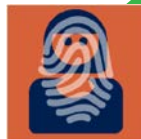
⁷ Information retrieved from Microsoft

LAW ENFORCEMENT

Project Vic is an image (and video) hash-sharing initiative that is used by law enforcement and led by the International Centre for Missing and Exploited Children (ICMEC). Using a database of millions of digital hashes of known child sexual abuse material, project Vic helps law enforcement distinguish already known images from unknown child sexual abuse material. This prevents copies of known images from having to be investigated again and enables detectives to focus on those images that are new and might involve children who still need to be identified. Thus Project Vic helps streamline investigative workflows. This is important given the increasing amount of data retrieved from offenders.



FACTS



Every image has a unique 'fingerprint'. Using clever mathematics - through the technology of PhotoDNA - each of these 'fingerprints' can be expressed as a unique numerical code which is commonly referred to as a 'hash'.

PhotoDNA is a technology that was first developed by Microsoft. Google is working on a tool that works similarly for videos, FMTS has already created such software.

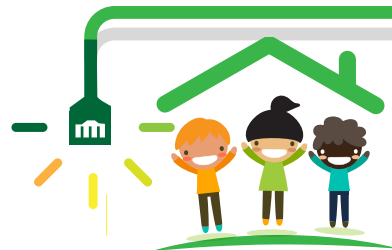


PhotoDNA is used to identify copies of known images without a human having to look at the images again.

The technology is used by law enforcement and organisations/ companies such as Google, Twitter and Facebook.

NOTE

The technology cannot be used to identify a person or object in an image, nor can it be used to reverse engineer and reconstitute an image.



INTERNET SERVICE PROVIDERS

The sets of hashes as created by PhotoDNA are also shared with Internet service Providers and Social network websites. The hash technology helps them detect child sexual abuse material shared on their services as it facilitates the processes of identification, removal or blocking and reporting of child sexual abuse material.



6 What is Cloud Computing?

And its implications for online child sexual exploitation

How Does it Work?

Traditionally, when people created something on a computer or wanted to store things like their music collection or pictures, they would have to put it on a hard drive or another medium such as a CD or USB stick. When you ran out of space, you had to buy or get additional hardware for storage. Similarly, if you wanted to run a programme, the software would have to be downloaded and installed on your device. If there was no room on the device, you could not use the programme.

The arrival of the Internet has completely changed that position. It has allowed for the development of cloud computing, often known as simply 'the cloud'. This means we can now use remote servers to store practically any amount of files or data and programmes or services can also be run on them. Because the

FACTS



Cloud services are instantly available for users (on demand) and are provided for free or on a pay-for-use basis.

Ever more services and personal data are moving into the cloud, such as e-mail (e.g. g-mail), pictures (e.g. Instagram), mobile phone applications, movies-on-demand (e.g. Netflix), banking services and server/ storage capacity.



Internet is global and always turned on, we now live in a world of mobile computing where everything we do can be backed up or stored on the cloud at any time.

The companies that offer the cloud service host the necessary infrastructure and applications and ensure its maintenance and security. Users can access the services over the Internet and all they need is a device, an Internet connection and a service account. This frees up users from having to buy, install or manage hardware and software on their personal computers.

Use of Cloud Services by Offenders

Offenders also utilise cloud services such as 'cyber lockers' or storage space online by uploading child sexual abuse material (CSAM) to 'their' locker. This locker is password-protected and its content can only be retrieved by logging into a personal account online. Offenders can share access to the content by providing the password or username for free or in exchange for CSAM or money. The company providing the service typically will have no knowledge of what is being stored inside the lockers.



This cloud storage space can be used e.g. by travelling child sex offenders who have created child abuse images abroad in order to reduce the risk of detection by the authorities. Instead of having to post or carry the material home, the offender uploads it to the cloud and accesses it upon return.

The emergence of cloud computing poses special challenges for law enforcement. This is partly due to the volume of files moving across the Internet and partly because a lot of this data is now encrypted.⁸

There are also jurisdictional issues: providers offering cloud services host the required physical infrastructure around the world, catering to clients from everywhere. This then poses difficulties in determining which jurisdiction law enforcement, online service providers and other parties are bound by, in case of investigation and prosecution.

8. Please see factsheet: What is Encryption?

7 What are Splash Pages?

And their deterrent value for child sex offenders online



How Does it Work?

A splash page is a page or image that appears over the entire screen or a portion of it while the web page sought by the user is loading.

Splash pages can be used for all kinds of purposes as they are a way of inserting a message onto a web page. Advertisers often use them to attract users or they can be used to tell you, for example, that you have typed an incorrect web address or that a particular web site no longer exists.

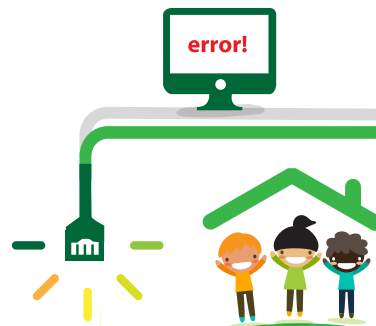
Splash pages are also used to keep users away from certain content. For example, a splash page can appear when someone is trying to access known child sexual abuse material (CSAM) and will obstruct access to the desired content as the final step in a deterrence scheme that involves filtering and blocking.⁹

Splash pages are used to attract users' attention, indicate a message or redirect users to other web pages.



Splash pages are used by non-governmental organisations, industry and law enforcement agencies.

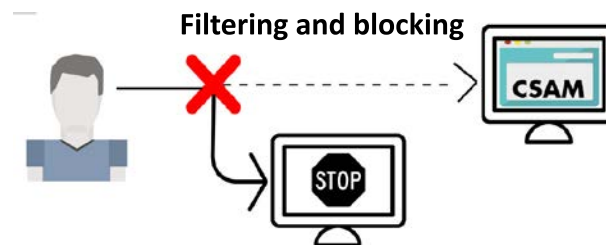
When splash pages are used to stop a user from accessing content, they are referred to as 'stop pages'.



9. For more information see factsheet: What is Filtering & Blocking?

Denying Access to Child Sexual Abuse Material

Splash pages are used by some companies - notably Microsoft and Google - in their search facilities as part of deterrence schemes intended to prevent people from intentionally or accidentally accessing child sexual abuse material online. Whenever someone attempts to access a page that is known to contain this type of material, the user will be denied access. When a splash page is used, the user will be subsequently redirected to a deterrence message.



Splash pages can contain varied information. The simplest version of a splash page contains a message indicating that access to the intended site has been denied. This is called an error-message or a 404-message. Splash pages can contain additional information as to why access has been blocked (with or without information about relevant legislation). This information can be complemented by a referral to sources of help or advice if a user is worried about his/her/other's sexual feelings towards children.

A splash page can also contain explicit warnings or messages explaining the illegality of the users' conduct or of the searched content. For users who do not agree with certain content being blocked, sometimes information on how to direct complaints about the denial of access is offered. Finally, some splash pages contain information and/or links to hotlines set up to report child sexual abuse content online.

By providing such information, splash pages can help build knowledge about the illegality of child sexual abuse material and related conducts. They can also help to instil a fear of being apprehended and redirect users to sources of help. Splash pages help to create a safer online environment by educating users about reporting mechanisms and by preventing unwanted exposure to such content. Ultimately, splash pages may deter users from accessing CSAM.

Please feel free to use the factsheets for your own work. All are available on www.ecpat.org under Resources > Factsheet > 2016-Factsheet.

The manifestations factsheets are available in Burmese, English, French, Indonesian (Bahasa), Khmer, Lao, Russian, Spanish, Thai, Turkish and Vietnamese.

The legal factsheets are available in English, French and Spanish.

The Internet and technology factsheets are available in Burmese, English, French, Indonesian (Bahasa), Khmer, Lao, Spanish, Thai and Vietnamese.



ECPAT International

328/1 Phaya Thai Road, Ratchathewi, Bangkok, 10400 THAILAND

Tel: +662 215 3388 Fax: +662 215 8272

Email: info@ecpat.org | Website: www.ecpat.org