Backing from
nominet trust
www.nominettrust.org.uk

Online Child Sexual Abuse Content: The Development of a Comprehensive, Transferable International Internet Notice and Takedown System

Dr. Weixiao Wei

The research project was funded by the Nominet Trust and the research report was written by an independent researcher, Dr. Weixiao Wei. The opinions, findings, and conclusions or recommendations expressed herein are those of the author and do not necessarily reflect those of the Nominet Trust, or any other organisations that participated the research project.

Table of Contents

List of Acronyms

ACMA	Australian Communications and Media Authority
BKA	German Federal Police (Bundeskriminalamt)
CAIU	Child Abuse Investigation Units
CEOP	Child Exploitation and Online Protection Centre
CEOS	Child Exploitation and Obscenity Section (the U.S. Department of Justice)
CGA	Civic Government (Scotland) Act 1982
CIRCAMP	COSPOL Internet Related Child Abusive Material Project
CJA	Criminal Justice Act of 1988
CJPOA	Criminal Justice and Public Order Act 1994
CP	Child Pornography
CSAC	Child Sexual Abuse Content
ECPAT	End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes
ESPs	Electronic Service Providers
FBI	Federal Bureau of Investigation of the U.S.
ICACs	Internet Crimes against Children Task Forces of the U.S.
ICAID	Interpol Child Abuse Image Database
ICCPR	the International Covenant on Civil and Political Rights
ICE	Immigration and Customs Enforcement (U.S. Department of Homeland Security)
ICSE DB	International Child Sexual Exploitation Image Database
INHOPE	International Association of Internet Hotlines
ISP	Internet Service Provider
IWF	Internet Watch Foundation
LKA	German State Police (Landeskriminalamt)
LSSICE	Spanish Information Society Services and Electronic Commerce Act 2002
MDStV	German Media Services State Treaty 1997 (Mediendienstestaatsvertrag)
MICT	Ministry of Information and Communication Technology

MoU	Memorandum of Understanding
NCMEC	National Centre for Missing & Exploited Children of the U.S.
NIM	National Intelligence Model
OCSET	Australian Federal Police Online Child Sex Exploitation Team
PCA	Protection of Children Act 1978 (England and Wales)
PCPSOA	Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005
RC	Refused Classification
TDG	German Federal Teleservices Act (Teledienstegestz)
TMG	German Telemedia Act (Telemediengesetz)
UCCIS	UK Council for Child Internet Safety
UDHR	the Universal Declaration of Human Rights
USPIS	the Postal Inspection Service of the U.S.
USSS	the U.S. Secret Service
VGT	Virtual Global Taskforce

Acknowledgments

This report has been produced with the financial assistance of the Nominet Trust; special thanks therefore go to them as the report could not have been possible without their generous contribution and support. Thanks also go to all the organisations that participated in the survey questionnaire and provided valuable feedback for the research. In particular, thanks go to the Internet Watch Foundation of the United Kingdom which assisted the research by providing guidance and resources, valuable feedback and comments, practical insights and recommendations.

Thanks are also owed to all the individuals who helped in various ways through the research, particularly Peter Robbins, CEO of the Internet Watch Foundation; Deborah McGovern, Deputy CEO and Director of Policy and Performance of the Internet Watch Foundation; Fred Langford, Director of Operations, Technology and Content of the Internet Watch Foundation; Steve Selves, Hotline Manager of the Internet Watch Foundation; Professor Ian Walden, University of London and Professor Alisdair A. Gillespie, De Montfort University.

Executive Summary

Pursuant to 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, child sexual abuse content (child pornography) is the representation of a child under 18 years old engaged in real or simulated explicit sexual activities or the representation of the sexual parts of a child for primarily sexual purposes.

Child sexual abuse content is regarded as one of harmful and illegal internet content in many countries and the availability and distribution of child sexual abuse content causes much concern in society. Whilst there have been collaborative international efforts to prevent and disrupt the circulation of online child sexual abuse content, how to effectively remove such content in order to protect internet users and minimise the impact on the physical and mental health, re-victimisation, safety and well-being of abused children has been hotly debated.

This report provides an in-depth analysis and evaluation of the existing legislative framework and regulatory regimes relating to online child sexual abuse content. The notice and takedown system relating to online child sexual abuse content is specifically examined along with other regulatory regimes including statutory regulation and Internet blocking.

The key findings identified are:

- The issue of online child sexual abuse content has been addressed at the international level through various international legal instruments; however, relevant law is not always clear and comprehensive at regional and national levels in order to guarantee protection of children from the crime of sexual exploitation on the internet.
- Regulatory regimes such as statutory regulation and self-regulation regarding online child sexual abuse content are established in several countries, although some are still at the stages of development.
- In terms of the removal of child sexual abuse content, statutory and non statutory bodies are permitted to issue notices to take down material in some countries and both legal entities such as law enforcement agencies as well as self-regulatory bodies operate. Statutory regulation is no longer the only mechanism for tackling child sexual abuse content given the extent of the problem. Internet blocking has a role in reducing the risk of exposure to online child sexual abuse content, particularly inadvertent access, and in the

reduction of re-victimisation of children, however, blocking access is controversial particularly in terms of the exercise of the right of users' privacy and freedom of expression. Blocking is not a panacea and it has the potential of being circumvented and if not technically deployed in a sophisticated way it can lead to over-blocking of legal material. Adequate safeguards are therefore required to ensure internet blocking is implemented proportionately and appropriately.

- There is compelling evidence that domestic notice and takedown systems adopted in some countries are beneficial in effectively removing child sexual abuse content at source without compromising the simultaneous capture of evidence necessary to investigate and prosecute offenders.
- The further development and effective implementation of an international notice and takedown system is considered to be important and beneficial, providing a number of influential but not exclusive issues are addressed. These include challenges posed by differing national legal standards relating to child sexual abuse content and the legal procedures relating to the takedown of such content; the impact of the development of an international notice and takedown system on the complex network of relationships on which international law enforcement co-operation relies; the impact of such an international notice and takedown system on the activities of law enforcement bodies and jurisdictional nuances as well as the risks to a national hotline organisation issuing international takedown notices.

Based on the findings identified, it is recommended:

- Harmonizing laws relating to online child sexual abuse content is essential for minimising the impact of different national standards on further development and effective implementation of an international notice and takedown system.
- A consistent and comprehensive international procedure for taking down child sexual abuse content needs to be developed, with due deference to applicable domestic and cross-border laws.
- Harmonization of practice and procedures between the organisations that issue international takedown notices is required in the development and implementation of an international notice and takedown system.
- The development of good partnerships between hotlines and law enforcement agencies should be encouraged so as to minimise the impact of an international notice and takedown system on law enforcement activity relating to child sexual abuse content and add value to law enforcement activities.

- Risk management strategies need to be developed and effectively implemented in order to minimise or provide cover for legal risk, reputation risk to the organisations that issue takedown notices and the risk of compromising law enforcement activity so that the organisations will not be impeded to issue takedown notices internationally.

Part 1: Introduction

1.1 Research Background

With the advance of the internet and digital technology, the availability and distribution of child sexual abuse content continues to raise concerns for society. This kind of content has a significant impact on the physical and mental health, re-victimisation, safety and well-being of children; the distribution of such content on the internet is therefore considered a serious crime in most countries.

Many countries have made efforts to combat illegal dissemination of child sexual abuse content, both by revising their domestic laws and reorganising their law enforcement resources in this regard. However, the policing of such content in a single country's internet territory can be problematic as the distribution of child sexual abuse content takes place on the internet crosses jurisdictional borders.

The current regulatory regime relating to child sexual abuse content comprises statutory regulation and self-regulation. Statutory regulation is established by law and enforced by law enforcement bodies. Self-regulation is developed by ISPs self-tailored technical mechanisms such as blocking or filtering for preventing access to child sexual abuse content or industry-wide codes of conduct. Another form of self-regulation often refers to hotlines operated by non-governmental organisations in co-operation with ISPs for reporting and taking down child sexual abuse content. Hotlines are initiatives for members of the public to report potentially criminal internet content. Hotlines may be operated by different types of organisation - industry, child welfare and public bodies and have varying functions and procedures depending on national legal and social circumstances. Among two regulatory approaches, hotlines providing a notice and takedown procedure to remove child sexual abuse content working in collaboration with ISPs and law enforcement bodies have shown to be effective by ensuring the expeditious removal of reported child sexual abuse content. It further has the advantages of providing intelligence to the police to identify child sexual abuse offenders or child victims. However, unless a close partnership exists between the various actors, risks of disturbing an ongoing surveillance operation could result in the loss of valuable evidence if adequate records are not maintained by service providers.

1.2 Research Objectives

Two hypotheses initiated the research. The first hypothesis is what role a notice and takedown system has played and should play in a strategy designed to achieve the

expeditious removal of internet child sexual abuse content, in particular, compared with other solutions such as statutory regulation and internet blocking. The second hypothesis is that if a notice and takedown system working in collaboration with law enforcement and ISPs is the preferred approach for the expeditious removal of internet child sexual abuse content, whether it can be transferred into an international context. Or, in other words, whether a global notice and takedown system can be developed in order to remove internet child sexual abuse content expeditiously?

With the hypotheses in mind, this report aims to examine the advantages and disadvantages of a notice and takedown system in effectively reducing online child sexual abuse content and to evaluate the potential of further developing a transferable international notice and takedown system for the expeditious removal of child sexual abuse content.

1.3 Research Methodology

The research looks into the development of a comprehensive, transferable international notice and takedown system relating to child sexual abuse content. A cross sectional analysis was employed to examine regulatory regimes relating to child sexual abuse content in several countries. The countries were chosen from different continents, including three European countries, two countries in the North and Latin America and three Asian-Pacific countries. Some of them have hotlines that are members of INHOPE, but others have hotlines that are not yet members of INHOPE. Both qualitative and quantitative research methods were used to collect information regarding child sexual abuse content by selecting examples of legislative and regulatory approach relating to such content from different jurisdictions, conducting interviews and survey questionnaires, etc. The information collected was then analyzed and interpreted to identify and compare the strengths and weaknesses of the existing notice and takedown system as well as the potential for further developing and implementing a notice and takedown system at an international level and what the barriers would be. Critical and comparative studies were applied to argue the role a notice and takedown system has played in a strategy designed to achieve the expeditious removal of internet child sexual abuse content and to further demonstrate the possibility of developing a global notice and takedown system in order to effectively eradicate online child sexual abuse content. The conclusion and recommendations of the report were drawn based on the critical and comparative analysis.

1.4 Outline of the Report

This research examines the existing notice and takedown system relating to child sexual abuse content in several different countries with a view to providing suggestions and recommendations for further development and effective implementation of a comprehensive, transferable notice and takedown system at the international level.

The study is structured as follows:

- Part 1 is an introduction to the report.
- Part 2 provides an overview of legislation and regulatory regimes relating to child sexual abuse content at the international and regional level as well as national level in several countries from different continents.
- Part 3 examines three main regulatory approaches relating to child sexual abuse content, including statutory regulation, notice and takedown system, and internet blocking. Strengths and weaknesses of the three regulatory approaches are discussed in detail.
- Part 4 addresses five influential factors in relation to further development and implementation of an international notice and takedown system.
- Part 5 presents the main conclusion from the research and makes recommendations for further development and implementation of a comprehensive, transferable international notice and takedown system.

It shall be noted that an in-depth discussion of an international notice and takedown system in this report by no means excludes or negates the need for other solutions to combat the circulation of child sexual abuse content on the internet. While the key to success relating to the eradication of child sexual abuse content around the world is a collaborative international effort, all other available solutions should be encouraged and considered to identify and remove child sexual abuse content from the internet.

1.5 Definition

Child sexual abuse content is a permanent record of the sexual abuse of a child and it can be presented in any format, such as, an image, an audio recording, a drawing, or a story about the sexual assault of a child. The terms "child pornography", "child porn" and "kiddie porn" are used in general language as well as in legislation, law-enforcement protocols, and by the media. The term “child sexual abuse content” is however used throughout the report rather than other terms except in the original

text of legislation quoted because it reflects more accurately the nature of the content. In addition, "child sexual abuse content" discussed in this report only refers to online child sexual abuse content but not those in an offline environment.

Part 2: Legal Approaches relating to Child Sexual Abuse Content Worldwide

2.1 Introduction

With the advancement of the internet and digital technology, the online distribution of child sexual abuse content has become a global issue and therefore receives considerable attention globally. There are several international instruments concerning child sexual abuse content as well as domestic laws that are in line with the requirements of the international laws. To effectively enforce the law and eradicate online dissemination of child sexual abuse content, many countries have also established statutory regulatory regimes by which the law can be implemented and enforced in order to combat child sexual abuse content related crimes and encouraged self-regulation in this regard.

To provide a cross sectional perspective of legal approaches on child sexual abuse content around the globe, this report will not only review international law and European law in this regard, it will also examine the domestic laws of several countries from different continents and the regulatory regimes relating to child sexual abuse content in these jurisdictions.

2.2 International Law and Development

Child sexual abuse content has been recognized as a global problem at international level and therefore several international policies have been made to address the problem by the United Nation. As the largest existing international organisation, with 192 Member States, the United Nations has conducted extensive research on the issues of child sexual exploitation and child sexual abuse content and developed international standards for protecting child from all forms of sexual exploitation and sexual abuse. Among those developments, the United Nation Convention on the Rights of the Child and the United Nation Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution, Child Pornography remain as the two most significant policies.

- **The 1989 United Nations Convention on the Rights of the Child**

As the first international instrument to incorporate the full range of human rights - civil, cultural, economic, political and social rights as they apply to children, the 1989 United Nations Convention on the Rights of the Child clearly states that children have

a right to protection from all forms of violence and abuse, including sexual exploitation and sexual abuse.

Firstly, in Article 1, the Convention provides definition of a child - a "human being below the age of 18 years unless under the law applicable to the child, majority is attained earlier".[1] Article 3 then stresses that States Parties are obliged to develop and undertake all actions and policies in the light of "the best interests of the child". In Article 19, the Convention further states that,

> States Parties shall take all appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse, while in the care of parent(s), legal guardian(s) or any other person who has the care of the child.

In terms of sexual exploitation and sexual abuse involving children, Article 34 explicitly states that States Parties are obliged to protect the child from all form of sexual exploitation and sexual abuse,

> States Parties shall in particular take all appropriate national, bilateral and multilateral measures to prevent the inducement or coercion of a child to engage in any unlawful sexual activity, the exploitative use of children in prostitution or other unlawful sexual practices, and the exploitative use of children in pornographic performances and materials.

- **The United Nations Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution, Child Pornography**

While child sexual abuse content is not defined in the 1989 United Nations Convention on the Rights of the Child, provisions in 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 complemented that. In the Optional Protocol, the definition of child sexual abuse content (child pornography) is given as "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".

[1] Despite the definition in the Convention and the fact that the age used in child sexual abuse related offences legislation in most cases is 18 years, definitional differences regarding age threshold still exist within different jurisdictions. Such differences are considered to be the obstruction of cross-border law enforcement operation relating to child sexual abuse content. See Yaman Akdeniz, Internet Child Pornography and the Law, (Aldershot, England: Ashgate, 2008), p.210.

The Optional Protocol supplements the 1989 United Nations Convention on the Rights of the Child by providing States with detailed requirements to combat sexual exploitation and abuse of children and protect children from being sold for non-sexual purposes. It serves as a comprehensive example of legal mechanisms that require states parties to prevent and combat sexual exploitation and abuse of children as well as provide and implement services to assist child victims and their families; in particular, it commits signatories to take measures to combat child sexual abuse content. Article 3(1) of the Optional Protocol creates obligation on State Parties to criminalize production, distribution, dissemination, importing, exporting, offering, selling or possession of child sexual abuse content, whether committed domestically or transnationally or on an individual or organized basis. In addition, Article 3(1) (c) requires State Parties to criminalise simple possession regardless of the intent to distribute. Furthermore, Article 3(4) addresses the liability of legal persons[2] and encourages each State Party to establish such liability for offences specific to child sexual abuse content, indicating the importance of industry involvement in the battle against child sexual abuse activities. In Article 10, paragraph 1, of the Optional Protocol, international co-operation is stressed and States Parties are required to promote international co-operation so as to prevent, detect, investigate, punish as well as address the root causes of, *inter alia*, child sexual abuse content and assist child victims because those illegal activities involving children are often transnational particularly with the advance of the internet and other evolving technologies.

- **Other Developments at the United Nations Level**

Following the 1989 United Nations Convention, the United Nations Commission on Human Rights decided to appoint a Special Rapporteur to consider matters in relation to the sale of children, child prostitution and child sexual abuse content. The Special Rapporteur is required to submit a report every year to the General Assembly of the United Nations presenting their findings and containing their conclusions and recommendations.

The Special Rapporteur's reports in 2004 and 2009 observed that although more than 137 of the United Nations Member States had ratified the Optional Protocol, the incomprehensive and ambiguous legislation on child sexual abuse content still "leaves

[2] Legal persons refer to non-human entities which have legal rights and are subject to obligations.

a dangerous gap that exposes children to the risk of abuse."[3] Given that countries have no borders where internet use is concerned, "coordinated, effective and structured international co-operation for the protection of all children"[4] worldwide is therefore of paramount importance in the Special Rapporteur's opinion. For this purpose, the reports called for increased international cooperation, including establishing an international mechanism for reporting internet-related offences.

2.3 The European Perspective

At a European level, there are several important policies to be considered:

- the Council of Europe Convention on Cybercrime
- the Council of Europe Convention on the Protection of the Children against Sexual Exploitation and Sexual Abuse
- the EU Council Decision of May 2000 to Combat Child Pornography on the internet
- the EU Council Framework Decision of December 2003 on Combating the Sexual Exploitation of Children and Child Pornography (also known as the Framework Decision 2004/68/JHA)
- the European Directive on Electronic Commerce
- the proposal for a Directive on Combating Sexual Abuse, Sexual Exploitation of Children and Child Pornography, repealing Framework Decision 2004/68/JHA[5]

Apart from the Convention on Cybercrime and Convention on the Protection of the Children against Sexual Exploitation and Sexual Abuse established by the Council of Europe. The European Union has also established several Directives and Decisions as effective tools for combating sexual exploitation and abuse of children because they give specific definitions of offences as well as provisions requiring punishment for

[3] Special Rapporteur (Mr. Juan Miguel Petit) Report of the Commission on the Sale of Children, Child Prostitution and Child Pornography, Rights of the Child, E/CN.4/2005/78, 23 December 2004, presented at the sixty-first session of the General Assembly of the United Nations, p.2.
[4] Special Rapporteur (Ms. Najat M'jid Maalla) on the Sale of Children, Child Prostitution and Child Pornography, Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, including the Right to Development, A/HRC/12/23, 13 July 2009, presented at the Twelfth session of the General Assembly of the United Nations, p.2.
[5] At the time of completing the report (January 2011), it is reported that the EU Council have decided their approach on this Directive and have agreed a text which will serve as the basis for the negotiations with the Parliament. The Council will send their negotiated text to the Parliament for examination. Afterwards, it will be sent back to the Council for a second reading. The full text of the Draft Directive 2010 is available at: http://www.statewatch.org/news/2010/nov/eu-council-sexual-exploitation-16958-10.pdf (last visited on 2 January 2011) and the origin text of the proposed Directive submitted by the European Commission on 29 March 2010 is available at: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/107 (last visited on 20 September 2010)

criminal behaviour. In addition, the European Directive on Electronic Commerce serves additionally as a legal mechanism for limiting ISPs' liability for illegal internet content. All the mechanisms allows for more effective prosecution of perpetrators.

In addition, implementation of several initiatives such as the Safer Internet Programme and the establishment of a number of organisations such as INHOPE are also of importance as they promote safer use of internet and tackle the problem of child sexual abuse content.

- **The Council of Europe Convention on Cybercrime**

The Council of Europe Convention on Cybercrime was established with the aim of implementing a cooperative and uniform approach to the prosecution of cybercrime and protecting legitimate interests in the use and development of information technologies. The Convention entered into force in July 2004 and laid down binding obligations for all governments wishing to develop legislation against cybercrime. Since it was not only open for signature by European states, but also open for signature by non-European states, the Convention provides a framework for international co-operation in the field of cybercrime and it is therefore deemed as the first international instrument on criminal offences committed through a computer system.

Pertaining to the area of child sexual abuse content, Article 9 (2) of the Convention states that child sexual abuse content shall include pornographic material that visually depicts a minor engaged in real or simulated sexually explicit conduct or any depiction of a minor's sexual organs for primarily sexual purposes. The definition of a "minor" is also given in paragraph 3 of Article 9 including all persons under 18 years of age though a State Party may require a lower age limit, which shall be not less than 16 years.

Article 9(1) recommends State Parties to make the following intended acts a criminal offence, including: "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; procuring child pornography through a computer system for oneself or for another person; and possessing child pornography in a computer system or on a computer-data storage medium".

Article 11 further requires State Parties to enact legislation necessary to address attempted crimes as well as aiding and abetting. Article 13(1) mandates State Parties to adopt legislative measures to ensure that criminal offences "are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty." In Article 12 (1), corporate liability is also addressed to hold legal persons liable for a criminal offence established in accordance with this Convention and committed for their benefit by any natural person such as an employee of the legal person. Article 23 then encourages international co-operation between countries in order to investigate or proceed criminal offences relating to computer systems and data, or to collect evidence in electronic form of a criminal offence.

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

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse is another effort made by the Council of Europe to prevent and combat sexual exploitation and sexual abuse of children and protect children against any form of sexual exploitation and sexual abuse through promotion of national and international co-operation. It was adopted and opened for signature at the 28th Conference of European Ministers of Justice held in Spain in 2007, and it was entered into force on 1st July 2010.

As a comprehensive legal instrument covering all relevant aspects of the protection of children against sexual exploitation and sexual abuse, the Convention defines child sexual abuse content ("child pornography") as "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."[6] In addition, Article 20(1) requires State Parties to criminalize acts of: producing child sexual abuse content; offering or making available child sexual abuse content; distributing or transmitting child sexual abuse content; procuring child sexual abuse content for oneself or for another person; possessing child sexual abuse content; and knowingly obtaining access, through information and communication technologies, to child sexual abuse content.

Article 21(1) also recommends State Parties to adopt legislation criminalizing the activities of those who recruit or coerce a child into participating in child sexual abuse content or knowingly attend performances involving child sexual abuse content.

[6] Article 20 (2) of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse

Similar to the provisions of the Council of Europe Convention on Cybercrime, this Convention addresses attempted crimes as well as aiding and abetting in Article 24 and corporate liability in Article 26(1). As for international co-operation in this field, Article 38(1) states that the Parties "shall co-operate with each other, in accordance with the provisions of this Convention, and through the application of relevant applicable international and regional instruments, arrangements agreed on the basis of uniform or reciprocal legislation and internal laws, to the widest extent possible," so as to prevent and combat sexual exploitation and sexual abuse of children, to protect and assist victims, and to investigate or proceed the offences established in line with this Convention.

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Abuse is the most recent international legal mechanism dealing with child sexual exploitation and sexual abuse, including child sexual abuse content. It "arguably constitutes the highest international standard for protecting children against sexual abuse and exploitation to date",[7] and at least provides clear common standards and definitions at the European level, in particular through harmonising criminal law and other relevant legislative measures.

- **The EU Council Decision of May 2000 to Combat Child Pornography on the Internet**

This decision was made soon after INHOPE was established in November 1999 and aimed to prevent and combat the production, processing, distribution and possession of child sexual abuse content on the internet.

Member States was required by the decision to take measures to encourage the reporting of child sexual abuse content and ensure law enforcement authorities react rapidly after receiving information on alleged cases of the production, processing, distribution and possession of child sexual abuse content. Measures may include the share of a list of 24-hour national contact points and specialised units between Member States in order to facilitate cooperation. In addition, Member States shall ensure that Europol, within the limits of its mandate, is informed of suspected cases of child sexual abuse content and shall examine the possibility of regular meetings between the national specialised services for exchanging information and promoting cooperation. The Decision also required the Member States to amend their criminal

[7] See Explanatory Memorandum of the Proposal for a Directive of the European Parliament and of the Council on Combating the Sexual Abuse, Sexual Exploitation of Children and Child Pornography.

procedural law in order to catch up with the technological developments which advances distribution of child sexual abuse content.

- **The EU Council Framework Decision of December 2003 on Combating the Sexual Exploitation of Children and Child Pornography (the Framework Decision 2004/68/JHA)**

The significance of the Council Framework Decision of December 2003 on Combating the Sexual Exploitation of Children and Child Pornography is that it provides an explicit definition regarding child sexual abuse content, which is:

> "pornographic material that visually depicts or represents: (i) a real child involved or engaged in sexually explicit conduct, including lascivious exhibition of the genitals or the pubic area of a child; or (ii) a real person appearing to be a child involved or engaged in the conduct mentioned in (i); or (iii) realistic images of a non-existent child involved or engaged in the conduct mentioned in (i)".

Additionally, the Decision made it clear that production, distribution, dissemination or transmission of child sexual abuse content as well as supplying or making available child sexual abuse content and acquisition and possession of child sexual abuse content is all illegal and punishable. The criminal and civil liability of legal persons is, *inter alia*, also established by the Decision as well as suggested sanctions.

Therefore, as the complement of several other related instruments such as the Council Decision of May 2000 to Combat Child Pornography on the internet in order to*, inter alia*, eradicate child sexual abuse content over the internet, this Framework Decision introduces a number of minimum rules for Member States' legislation to criminalise the most serious forms of child sexual abuse and exploitation. The Decision also addresses issues of jurisdiction and prosecution and provides for a minimum of assistance to victims.

Nevertheless, a number of shortcomings also exist in the Framework Decision. For example, only a limited number of offences were considered without addressing new forms of abuse and exploitation facilitated by the use of information technology. The Framework Decision does not remove obstacles to investigating and prosecuting offences in cross-border cases. In terms of protection of child victims, provisions of the Framework Decision are not sufficient to meet all the specific needs of child victims. In addition, adequate measures to prevent offences are lacked in the

Framework Decision.[8] Due to those deficiencies, the European Parliament and the Council of the European Union have recently proposed a new Directive on Combating the Sexual Abuse, Sexual Exploitation of Children and Child Pornography,[9] which will be discussed later. If this proposed Directive is finally adopted, it will repeal this Framework Decision 2004/68/JHA.

- **The European Directive on Electronic Commerce**

To ensure the free movement of "information society services" across the European Community, the European Union adopted the Directive on Electronic Commerce on 8th June 2000. Apart from provisions dealing with the establishment of service providers, commercial communications, electronic contracts, codes of conduct, out-of-court dispute settlements, court actions and co-operation between Member States, the Directive also contains provisions on liability of service providers.

According to the Directive, liability of service providers is a limited and notice-based liability regime with takedown procedures for illegal internet content. Therefore, service providers are liable only if they, acting as a host provider, have actual knowledge of illegal activity or content and fail to remove or to disable access to the information concerned.[10] They are not liable if their activity is of a mere technical, automatic and passive nature, which implies that the service provider has no knowledge of or control over the information which is transmitted or stored;[11] or if

[8] See the Proposal for a Directive of the European Parliament and of the Council on Combating the Sexual Abuse, Sexual Exploitation of Children and Child Pornography, repealing Framework Decision 2004/68/JHA submitted by the Commission to the Council on 29 March 2010, available at: http://www.europarl.europa.eu/oeil/file.jsp?id=5763632

[9] See *supra* note 5.

[10] Article 14: Hosting
1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.
2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.
3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

[11] Article 12: "Mere conduit"
1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:
(a) does not initiate the transmission;
(b) does not select the receiver of the transmission; and
(c) does not select or modify the information contained in the transmission.

their activity is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored.[12]

However, the limitation on service providers' liability does not affect the possibility of a court or administrative authority, in accordance with Member States' legal systems, requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it.[13]

Nevertheless, apart from the exception that "this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation",[14] Member States are prohibited by the Directive from imposing a general monitoring obligation on service providers, including monitoring the information which they transmit or store, or seeking facts or circumstances indicating illegal activity.[15]

The impact of the Directive on Electronic Commerce on liability of service providers for child sexual abuse content at the European level,[16] therefore, is that service providers are liable only if they fail to remove or to disable access to the content upon obtaining actual knowledge of child sexual abuse content. Nonetheless, with regard to procedures governing the removal or disabling of access to illegal information (content), the Directive encourages self-regulatory solutions and procedures to be developed by the internet industry to implement and bring into

---

2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.
3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

[12] Article 13: "Caching"
1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:
(a) the provider does not modify the information;
(b) the provider complies with conditions on access to the information;
(c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
(d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
(e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

[13] Article 12 (3), 13 (2), and 14 (3) of the Directive on Electronic Commerce

[14] See Recital 47 of the Directive on Electronic Commerce

[15] Article 15 (1) of the Directive on Electronic Commerce

[16] European Member States had until 16 January 2002 to implement the Directive on Electronic Commerce into national law whereas the final implementation in many Member States was slightly delayed.

action notice and takedown procedures, instead of regulating it in the Directive itself.[17]

- **The Proposal for a Directive on Combating the Sexual Abuse, Sexual Exploitation of Children and Child Pornography**

As mentioned above, the Directive of the European Parliament and of the Council on Combating the Sexual Abuse, Sexual Exploitation of Children and Child Pornography is proposed to recast Framework Decision 2004/68/JHA on the sexual abuse, sexual exploitation of children and child sexual abuse content by including new provisions aimed at making it more effective.

Pertaining to child sexual abuse content, a number of provisions[18] are adopted and checked in particular with regard to freedom of expression (Article 10 of the European Convention on Human Rights, Article 11 of the Charter of Fundamental Rights of the European Union) in order to increase law enforcement activities to combat crimes of publishing and disseminating child abuse material, advertising child sexual abuse content or encouraging child sexual abuse. Mechanisms to restrict access to internet pages containing and disseminating child sexual abuse content are also proposed.

For instance, according to the latest version of the draft Directive by the end of 2010, in Article 2 (b), definition of child sexual abuse content (child pornography) is amended to refer to "(i) any material that visually depicts a child engaged in real or simulated sexually explicit conduct; or (ii) any depiction of the sexual organs of a child for primarily sexual purposes; or (iii) any material that visually depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of any person appearing to be a child, for primarily sexual purposes; or (iv) realistic images of a child engaged in sexually explicit conduct or realistic images of the sexual organs of a child, for primarily sexual purposes".

This makes the definition of child sexual abuse content in this Directive approximate to that of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse and the Optional Protocol to the Convention on the Rights of the Child. According to Article 5, acquisition, possession, production, distribution, dissemination or transmission of child sexual abuse content; knowingly obtaining access, by means of information and communication technology, to child

[17] See Recital 40 and Article 16 of the Directive on Electronic Commerce.
[18] See recital 13 of the proposed Directive.

sexual abuse content; offering, and supplying or making available child sexual abuse content shall be punishable by imprisonment from minimum of one year and up to maximum of five years. But the Member States have the right to decide whether Article 5 applies to cases involving child sexual abuse content, as referred to in Article 2(b)(iii), where the person appearing to be a child was in fact 18 years of age or older at the time of depiction.

The Member States also have the discretion to decide whether the above-mentioned activities "apply to cases where it is established that pornographic material as defined in Article 2(b) (iv) is produced and possessed by the producer solely for his or her own private use, as far as no pornographic material as referred to in Article 2(b)(i) to (iii) has been used for the purpose of its production, and provided that the act involves no risk of dissemination of the material."

Liability of, and sanctions on, legal persons for child sexual abuse content are also addressed in Article 11 and 12. These require Member States to take the necessary measures to ensure that legal persons may be held liable for, *inter alia*, child sexual abuse content referred to in Article 5. Article 21 then requires Member States to "take necessary measures to ensure the removal of webpages identified as containing or disseminating child sexual abuse content hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory."

Where the removal of webpages containing or disseminating child sexual abuse content is not possible, Member States shall take the necessary measures, either legislative or non-legislative, to block access to webpages that contain or disseminate child sexual abuse content in their territory, while providing adequate safeguards to relevant parties such as internet users and content providers. Despite opinions being divided among Member States regarding blocking, in particular, obligatory blocking, the expectation of the Directive is that blocking and removal at source work together to make a real difference in minimising the availability and circulation of child sexual abuse content over the internet through whatever measures necessary - legislative or non-legislative.

At the end of 2010, the proposal had gone through the European Council and will be sent to the European Parliament for examination. It was noted that the proposed Directive aims to "further approximate national legislation and to improve international law enforcement and judicial cooperation." Among the outstanding issues are: the definition of child sexual abuse content (child pornography); the criminalisation of intentional access to child sexual abuse content by computerised

means; the blocking of websites with child pornography content as a complementary measure to the efforts to eliminate the source content; and the inclusion of unreal characters (images, cartoons, etc.) within the concept of child sexual abuse content.

- **Other Developments at the EU Level**

In addition to the legislation discussed above, a number of initiatives are carried out in Europe with the aim of promoting safer use of the internet and new online technologies, particularly for children, and fighting against illegal content including online child sexual abuse content. The Safer Internet Programme and INHOPE funded by the Safer Internet Programme deserve special mention.

The Safer Internet Programme

The Safer Internet Programme is an initiative of the European Commission to fund activities that fight and prevent illegal and harmful content. The programme has been running since 1999 and it has four main actions:

(a) setting up a European network of hotlines for reporting illegal and harmful content;

(b) encouraging self-regulation initiatives in this field and involve children in creating a safer online environment;

(c) developing content rating and filtering, benchmarking filtering software and services; and

(d) raising public awareness of safer use of the internet.

To date, the Safer Internet Programme has funded Safer Internet Centres in 27 European countries, among them, the Internet Watch Foundation (the IWF) of the UK, the Protegeles hotline of Spain and several German hotlines.

INHOPE (the International Association of Internet Hotlines)

INHOPE was founded in 1999 as part of the European Commission Safer Internet Action Programme and is funded by the Safer Internet Programme. While illegal activity on the internet is a cross border problem and a single hotline can only be successful at tackling the problem on a national level, international corporation is needed when content is hosted in a foreign country or the perpetrator is located abroad. With this in mind, the aim of INHOPE is therefore to coordinate and facilitate the work of internet hotlines in responding to illegal and harmful use of the internet in order to eliminate child sexual abuse content from the internet and protect young people from harmful and illegal uses of the internet.

At present, INHOPE represents and co-ordinates the global network of 39 internet hotlines in 34 countries worldwide, which allow members of the public to report certain contents they suspect to be illegal on the internet (specific content depending on which country the hotline is based in). When reports reach hotlines, the hotline will investigate these reports to determine if they are potentially illegal based on its domestic law, and if so, the hotline will trace the origin of the content. When the content is deemed potentially illegal, the hotline will refer the report onto law enforcement agencies in the country and/ or also the internet service provider for removal of the content depending on the national agreement. When material reported to Hotlines is hosted beyond the borders of their own countries or the perpetrator is located abroad, the report will be passed over to hotlines in the relevant countries for action, or through the law enforcement path. With regard to exchange of reports on illegal contents, INHOPE members have set processes in place to ensure rapid and effective response to reports of illegal content. So far, majority of INHOPE member hotlines have the support of their national government, internet industry, law enforcement, and internet users in the countries of operation and offer effective transparent procedures for dealing with complaints.

According to INHOPE statistics[19], from the period of September 2005 to March 2010, about 46,100 reports have been made to INHOPE member hotlines every month. There were 42 per cent of the reports being assessed by hotline staff as illegal in which 48 per cent were related to child sexual abuse content. The statistics also indicated that "the number of reports received externally by INHOPE hotlines is on a statistically significant increasing trend, at an average rate of +280 reports per month."

2.4 Perspectives of Different Countries

The panorama of the legal approach to child sexual abuse content on the internet at the national level differs from country to country. However, no matter which legal system is in place, child sexual abuse content related offences are criminalised in either the criminal code or the laws aimed to protect children. Regulatory regimes relating to child sexual abuse content offences are also established with full support of the law enforcement agencies and collaboration of the internet industry in many countries.

[19] See INHOPE, Trend Analysis Update (March 2010).

This part aims to examine national legislation and regulatory regime of several countries from different continents in order to provide a cross sectional analysis of legal framework relating to online child sexual abuse content around the globe.

2.4.1 European Countries: the UK, Spain, and Germany

2.4.1.1 The United Kingdom

A comprehensive legislative and regulatory regime relating to child sexual abuse content is established in the UK to combat online sexual abuse content. Specific legislation concerning liability for child sexual abuse content was introduced and has been updated in line with international law and European legislation. A self-regulated notice and takedown system has also been developed for the effective removal of child sexual abuse content under the operation of the national hotline – the IWF.

UK Legislation

In England and Wales, the main piece of legislation pertaining to child sexual abuse content is the Protection of Children Act 1978 (England and Wales) (the PCA 1978) as amended by several other Acts to respond to new offences and the impact of digital technology. In Scotland, the Civic Government (Scotland) Act 1982 (the CGA 1982) as amended by Section 16 of the Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005 (the PCPSOA 2005) is the main statute dealing with child sexual abuse content. As for liability of internet service providers for child sexual abuse content, the Electronic Commerce Regulation 2002 is the one that provides certain exemptions for ISPs that have no knowledge of illegal information activity and no control of it.

- **The PCA 1978**

The PCA 1978 is the main act dealing with child sexual abuse content offences in England and Wales. It aims to prevent the exploitation of children by making indecent photographs of them; and to penalise the distribution, showing and advertisement of such indecent photographs. Since 1978, the PCA 1978 has been amended several times by

- the Criminal Justice Act of 1988 (the CJA 1988) (introducing the possession offence),
- the Criminal Justice and Public Order Act 1994 (the CJPOA 1994) (introducing the concept of computer generated pseudo-photographs),

- the Criminal Justice and Court Services Act 2000 (extending the maximum imprisonment sentences for child sexual abuse content related offences),
- the Sexual Offences Act 2003 (amending the definition of a child e.g. age threshold to bring it into line with international law), and
- the Criminal Justice and Immigration Act 2008 (amending the definition of indecent photography of children to include computer generated photography and images of children).

Pursuant to the Act, it is a criminal offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children.

Despite this, there is no legal definition of the term "child pornography" to be found in any legislation dealing with child sexual abuse content related offences, whereas the provisions relating to indecent photography and pseudo-photography (since the Act was amended by the CJPOA 1994) of children offences within the PCA 1978 are referred to as offences of child sexual abuse content.

Originally, a child was described as a person under 16 years of age by Section 7 (6) of the PCA 1978. However, the age threshold has been redefined and changed to a person under the age of 18 when the PCA 1978 was amended by the Sexual Offences Act 2003.[20] Limited defences[21] are provided for in cases where the child is 16 or over and the defendant is the child's partner or married to the child and the photograph must not be one that shows a person other than the child and the defendant. This change of age threshold indicates the offences in relation to taking, making, permitting to take, distributing, showing, possessing with intent to distribute, and advertising indecent photographs or pseudo-photographs of children will be applicable where the photographs concerned are of children of 16 or 17 years of age. The same change applies to the offence of possessing an indecent photograph or pseudo-photograph of a child under section 160 of the CJA 1988 (section 160(4) applies the PCA 1978 definition of "a child").

As far as the definition of indecent photography of children is concerned, for the purpose of both Section 7 (4) of the PCA 1978 and Section 84 (4) of the CJPOA 1994, photography includes the negatives as well as the positive version, and data stored on a computer disc or by other electronic means which is capable of conversion into a

[20] See Section 45(2) of the Sexual Offences Act 2003.
[21] See Section 45(3) of the Sexual Offences Act 2003, which sets out a number of conditions which if satisfied will exempt the defendant from an offence under section 1(1)(a), (b) or (c) of the 1978 Act (provided that the offence charged relates to a photograph and not a pseudo-photograph) and an offence in relation to the possession of indecent photography of a child under Section 160 of the Criminal Justice Act of 1988.

photograph. With regard to definition of pseudo-photograph, references to a pseudo-photograph include an image, whether made by computer-graphics or otherwise, which appears to be a photograph, for the purpose of both Section 7 (4) of the PCA 1978 and Section 84 (4) of the CJPOA 1994. However, with more and more digital images as well as computer generated images of children becoming available and circulated over the internet, further clarification was required to redefine indecent photography of children in the backdrop of technology advancement. In Section 69 of the Criminal Justice and Immigration Act 2008, definition of indecent photographs of a child under 18 years of age was amended to include:

> (a) A tracing or other image, whether made by electronic or other means (of whatever nature)
>
> (i) which is not itself a photograph or pseudo-photograph, but
> (ii) which is derived from the whole or part of a photograph or pseudo-photograph (or a combination of either or both); and
>
> (b) data stored on a computer disc or by other electronic means which is capable of conversion into an image within paragraph (a); and subsection (8) applies in relation to such an image as it applies in relation to a pseudo-photograph.

Simple possession of indecent photographs and/or pseudo-photography of a child under the age of 18 were made arrestable offences carrying a maximum sentence of five years imprisonment by Section 160 of the CJA 1988 unless the defendant satisfies one of three conditions: legitimate reason, knowing possession, and unsolicited photographs or pseudo-photographs listed in Section 160 (2) of the CJA 1988.

Apart from the offences given by Section 1 of the PCA 1978, the CJPOA 1994 amended Section 1 of the PCA 1978 to include an offence of "making" indecent photographs or pseudo-photographs of a child under 18 years of age. Based on the court ruling of *R v. Bowden*[22] and *R v. Smith & Jayson*[23], downloading indecent images of children from the internet as well as storing them on the computer or printing them out is another serious arrestable offence of "making" an indecent image of a child, which will carry a maximum sentence of ten years imprisonment.

[22] See *R v. Bowden* [2000] 2 All ER 418 in which the Court of Appeal held that the downloading and/or printing out of computer data of indecent images of children from the internet was capable of amounting to a "making" offence within the meaning of Section1 (1) (a) of the Protection of Children Act 1978.
[23] See *R v. Smith & Jayson* (CA, [2002] EWCA Crim 683) in which the Court of Appeal ruled that "the act of voluntarily downloading an indecent image from a web page on to a computer screen is an act of making a photograph or pseudo-photograph".

- **The CGA 1982 and its Amendments**

In Scotland, indecent child photographs are also deemed illegal. Pursuant to Section 52 of the CGA 1982 as amended by Section 16 of the PCPSOA 2005, it is an offence for a person

- to take, or permit to be taken, or to make any indecent photographs or pseudo-photographs of a child under age 18; or
- to distribute or show such indecent photographs or pseudo-photographs; or
- to possess such indecent photographs or pseudo-photographs, with a view to their being distributed or shown by himself or others; or
- to publish or cause to be published any advertisement likely to be understood as conveying that the advertiser distributes or shows such indecent photographs or pseudo-photographs, or intends to do so.

Possession of such indecent photographs or pseudo-photographs of a child under 18 years of age also constitutes an offence under Section 52A of the CGA 1982 as amended by the PCPSOA 2005. Similar to the English case law, downloading indecent child sexual abuse images from the internet is deemed as "making" such content in line with Section 52(1) (a) of the CGA 1982.[24]

Certain exemptions for photographs of 16 and 17 year olds are given by Section 52B of the CGA 1982 as amended by the PCPSOA 2005, for example, if the accused proves that

(a) either the photograph in question was of the child aged 16 or over; or the accused reasonably believed that to be so;
(b) at the time of the offence charged or at the time when the accused obtained the photograph, the accused and the child were married; or are partners in an established relationship, and
(c) either the child consented to the photograph's being taken or made; or the accused reasonably believed that to be so.

In addition to the above conditions, the exemption would only apply for an offence of distributing or showing indecent photographs or pseudo-photographs under Section 52(1) (b) if the showing or distributing of the photograph was only to the child alone.

[24] See *Longmuir v. H.M.A*. 2000 S.C.C.R. 447 in which the Appeal Court held that downloading images from the Internet was within Section 52(1)(a). The word "make" covered an activity whereby a computer was used to bring into existence data stored on a computer disk. A person who downloads images is therefore making photographs. Operation of a computer to download electronic signals could be distinguished from mere possession of indecent photographs (where the possessor has not himself been responsible for bringing the material into existence).

The exemption would only apply for an offence of possessing indecent photographs or pseudo-photographs with a view to its being distributed or shown by himself or others under Section 52(1) (c) if the above conditions were satisfied and the accused had the photograph in his possession with a view to its being distributed or shown only to the child.

- **The Electronic Commerce (EC Directive) Regulations 2002**

To implement the European Directive on Electronic Commerce into the UK law, the Electronic Commerce (EC Directive) Regulations 2002 came into force. Among other things, the Regulations provide liability of online service providers for illegal information and activity including those relating to child sexual abuse content.

The UK Regulations transposed most of the provisions of the Directive on Electronic Commerce in particular those in relation to ISP liability. Provisions of the Directive in relation to ISP liability for mere conduit, caching and hosting are provided by regulations 17, 18 and 19 of the 2002 Regulations. The provisions with regard to notice and takedown procedure are incorporated in regulations 19 on hosting activity. Liability of an ISP under regulations 19 (a) is established only if (i) the ISP has actual knowledge of unlawful activity or information and, where a claim for damages is made, is aware of facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful; or (ii) upon obtaining such knowledge or awareness, the ISP does not act expeditiously to remove or to disable access to the information.

Nevertheless, Article 15 of the Directive regarding "no general obligation to monitor" has not been transposed into the 2002 Regulations due to the government concern that such provision "would not only confer no additional legal certainty on intermediaries but could even introduce uncertainty if the prohibition were interpreted differently from its meaning in the Directive."

The Regulations do not provide any statutory notice and takedown procedure for the removal of illegal internet content, industry self-regulation along with development of industry-wide codes of conducts in this regard are the emphasis of the government.

As far as ISP liability for child sexual abuse content is concerned, the impact of the 2002 Regulations is that the UK ISPs are encouraged to develop self-regulatory rules and codes of conduct on combating child sexual abuse content over the internet. However, an ISP would be subject to liability for child sexual abuse content if it has

actual knowledge or awareness of the availability of such illegal content (being notified the existence of such material on his servers) and fails to take prompt action to remove or disable access to the content.

UK Regulatory Regime

As mentioned, the UK has a comprehensive legal framework around child sexual abuse content and the police would, in accordance with the law[25], act against any individuals or organisations who take, permit to be taken, make, possess, show, distribute or advertise child sexual abuse content or facilitate the above-mentioned activities concerning child sexual abuse content. However, with growing availability and widespread circulation of child sexual abuse content over the internet, co-operation between government and the ISP industry has also been encouraged to combat such illegal content, in which the ISP industry would develop self-regulatory mechanisms for reporting child sexual abuse content in order for the content to be finally taken down and for the suspects to be prosecuted.

In 1996, the IWF was established as the direct result of discussion and campaign on ISPs' involvement in fighting against illegal internet content, in particular child sexual abuse content. The IWF is currently funded by the European Union and the wider online industry, including internet service providers, mobile operators and manufacturers, content service providers, filtering companies, search providers, trade associations and the financial sector as well as other organisations that support them for corporate social responsibility reasons. It works in partnership with the online industry, law enforcement, government, and international partners such as the INHOPE member Hotlines.

Under the self-regulatory regime, a national hotline is provided by the IWF for the public and IT professionals to report potentially illegal internet content including child sexual abuse content as well as other illegal content within the remit of the IWF. Therefore, the IWF acts as the "notice and takedown" body in the UK for the afore-mentioned content.

Where the material is hosted within the UK, the IWF will attempt to trace the source of origin, and assess if the content is potentially illegal pursuant to the provisions of

[25] It mainly refers to the Protection of Children Act 1978 for the police to prosecute the offenders and Section 39 of the Police and Justice Act 2006 and Schedule 11 to the Act amend the Protection of Children Act 1978, which came into effect on 1 April 2008, for the police to forfeit indecent photographs of children held by the police following any lawful seizure.

relevant law[26], and make request for the removal of the illegal content. The IWF refers the report to their police partners, such as the Child Exploitation and Online Protection Centre (CEOP) in the case of child sexual abuse content so that the police can instigate an investigation if needed. By working with relevant service providers and British law enforcement, the IWF will try to ensure that the content has been evidentially preserved and then subsequently being taken down. The IWF will also assist wherever operationally possible to have the offender(s) responsible for the illegal content detected.

In the case of illegal material originated outside the UK, the IWF reports the content to the CEOP who in turn would pass the information onto Interpol who (in theory) pass it on to the relevant police authority. The IWF also passes details of every identified non-UK website to their partner hotline in that country so they can investigate it within their own legislation and in co-operation with their national law enforcement agencies. In some cases where there is an agreement between the IWF and that country's hotline, the IWF will approach the ISP directly. An example of this is the case of co-operation between the IWF and the National Centre for Missing and Exploited Children of the U.S. (NCMEC) in that the IWF will, after agreed amount of time of notifying NCMEC, contact the hosting American ISP identified in the report via email with every correspondence being copied to a dedicated NCMEC email box for their information. The IWF then monitors the removal of the content on the particular site while the IWF simultaneously notifies the NCMEC by reporting the existence of the content through an automated facility available for IWF use.

To protect UK internet users from inadvertent exposure to illegal content, whilst liaison with other hotlines and/or law enforcement agencies is ongoing, the IWF maintains a dynamic blacklist of internet sites and content that it deems to be in contravention/potentially in contravention to UK laws. The list consists of what is considered child sexual abuse content URLs for voluntary download to its licensees that have the ability to filter and block access to such content hosted in the UK and beyond the UK jurisdiction. National and international law enforcement agencies and the INHOPE Hotlines may also access to the list on a mutual exchange basis.[27] By now, about 98.6% of the UK ISPs have adopted the IWF blacklist to block access to potentially illegal content hosted abroad.[28]

[26] It refers to, in particular, the Sentencing Guidelines Council's Definitive Guidelines of the Sexual Offences Act 2003.
[27] See " IWF Facilitation of the Blocking Initiative", available at http://www.iwf.org.uk/public/page.148.htm
[28] See, A Campbell, Hansard HC vol 497 col 1546W (21 Ocotober 2009), available at

2.4.1.2 Spain

As one of the top 5 countries hosting images of child sexual abuse,[29] Spain has criminalised several offences relating to child sexual abuse content in its Penal Code and set up both police and non-police hotlines for reporting child sexual abuse content.

Spanish Legislation

In Spain, the Spanish Penal Code is the main statute that deals with child sexual abuse content offences whereas the LSSICE regulates ISPs' liability for online child sexual abuse content offences.

- **The Spanish Penal Code**

Child sexual abuse content offences are covered by Article 189 of the Spanish Penal Code. Article 189 of the Spanish Penal Code defines prohibited and punishable activities relating to child sexual abuse content.

Article 189(1) (a) explicitly states that it is a criminal offence to use under-age or incapable persons to "prepare any type of pornography material". Pursuant to the provision of Article 189(1) (b), it is illegal to produce, sell, distribute or exhibit, or facilitate production, sale, distribution or exhibition of pornographic material of under-age or incapable persons "by any means". Penalty also applies to computer-facilitated offences relating to child sexual abuse content. A person under 18 years of age is considered as under-age by the Spanish law while the definition of "a child" is given by the 1989 United Nations Convention on the Rights of the Child and the European Convention on Cybercrime to which Spain is a signatory country. 13 years old is the age threshold for the age of consent according to Article 181 (2) of the Spanish Penal Code.

Knowingly possessing child pornographic material for any of the above-mentioned purposes is also illegal, though simple possession receives lower penalty.[30] Pursuant to the Penal Code, higher penalties will be given to the offender who is a member of an organisation or association, either run temporarily or for a long time, which is dedicated to such activities.

---

http://www.publications.parliament.uk/pa/cm200809/cmhansrd/cm091021/text/91021w0024.htm (last visited on 22 September 2010)

[29] See Child Sexual Abuse Images: An Analysis of Websites by Cybertip!Ca, November 2009, p.26

[30] When a new law came into force reforming the Spanish Penal Code in October 2004, possessing child pornography material was introduced as a crime.

Nevertheless, no definition is given to the term of "child pornography" [31] by the Spanish law, although the definition of such a term is given by the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. Spain has been a signatory country since March 2009, but has not yet ratified the Convention. Therefore, "in many cases it is still difficult to determine with sufficient certainty whether a given image should be considered child pornography or not."[32]

- **LSSICE (Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico - Law 34/2002 of 11 July, Services of Information Society and Electronic Commerce)**

The European Directive on Electronic Commerce was transposed into Spanish national law through the Information Society Services and Electronic Commerce Act 2002 (Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico - hereinafter the LSSICE).[33] The LSSICE sets forth ISP liability exemptions for illegal activity and information in Articles 14 (mere conduit), 15 (caching) and 16 (hosting). In addition, the Spanish law establishes a safe harbour for the provision of hyperlinks and information location tools in Article 17, with the same requirements as the liability exemption for hosting. However, as to what constitutes "actual knowledge", the LSSICE has a restrictive definition of "actual knowledge" of ISPs in relation to liability exemption for hosting and hyperlinks and information location tools[34] while only a previous decision declaring the illegality of the materials might be qualified according to several case laws[35].

Article 18 sets forth provisions relating to codes of conducts in which development and implementation of voluntary codes of conduct on combating illegal online are encouraged, in particular, procedures for the detection and removal of illegal content.

---

[31] See the International Centre for Missing and Exploited Children (ICMEC), "Child Pornography: Model Legislation & Global Review", 2010, 6th Edition, available at http://www.icmec.org/en_X1/icmec_publications/English__6th_Edition_FINAL_.pdf (last visited on 2 May 2011), p.30.

[32] See Protegeles, "Child Pornopgrahy", 1.3.3 Illegal Activities, available at http://www.protegeles.com/eng_linea1.asp

[33] Law 34/2002 of 11 July 2002 of "Servicios de la Sociedad de la Información y de Comercio Electrónico", BOE (Spanish Official Journal) no.166, July 12, 2002. The law came into force on October 12, 2002 and has been modified on several occasions. The official text and all the amendments are available in Spanish at http://www.lssi.es/Secciones/Normativa/ (last visited on April 29, 2008).

[34] Article.16.1.II of the LSSICE states that, "it will be understood that the service provider has the actual knowledge referred to in paragraph (a) when a competent body has declared that the data are unlawful, or has ordered their removal or the disablement of access to them, or the existence of the damage has been declared, and the provider knew of this resolution, without prejudice to the procedures of detection and removal of content that providers may apply by virtue of voluntary agreements, and without prejudice to other means of actual knowledge that might be established." The same paragraph appears in Article.17 of the LSSICE, which sets forth a liability exemption for the provision of links and search engines--which was not included as a safe harbour in the Directive on Electronic Commerce.

[35] Miquel Peguera, "'I Just Know that I (Actually) Know Nothing': Actual Knowledge and Other Problems in ISP Liability Case Law in Spain", *E.I.P.R.* 2008, 30(7), pp.280-285, p.282

The transposition of the Directive on Electronic Commerce into the Spanish law suggests that, Spanish ISPs' liability for child sexual abuse content will be established only if the ISPs fail to remove or disable access to child sexual abuse content expeditiously upon their actual knowledge of such content.

Regulatory Regime in Spain

Apart from the hotline set up by the Spanish Police for investigating and prosecuting child sexual abuse content offences, another regime dealing with such content is the hotline operated by Protegeles - a Spanish non-profit organization for reporting illegal content on the internet, especially child sexual abuse content. Protegeles is mainly funded by the Safer Internet Program of the European Union and is supported by the Spanish government, in particular, the Spanish Law Enforcement Units and several Spanish Ministries such as Industry, Tourism and Commerce Ministry (Ministry of Science and Technology previously) and Child Ombudsman.

The Protegeles hotline has been operating since October 2001 and it is the only non-police hotline dealing with child sexual abuse images in Spain. The hotline works closely with major Spanish ISPs, law enforcement, government, and other international organizations such as INHOPE. Additionally, the Protegeles hotline has set up several joint hotlines together with Latin-American hotlines from countries of Peru, Costa Rica and Argentina.

Similar to the UK IWF model, the hotline operated by Protegeles receives reports from the public about unlawful internet content and then traces the origin of the content. Once the origin of the content is located the hotline will inform the Spanish Police Brigade for Technology Investigation (Technology Research Squad - BIT on its Spanish acronym) or the Guardia Civil Group for Technologic Crimes (the Guardia Civil Telematics Offences Squad) about the potentially illegal content for possible criminal investigation and prosecution. For the swift and effective removal of the unlawful content, the hotline also informs ISPs that hosted the content and collaborates with the law enforcement agencies to fight against child sexual abuse content. Nevertheless, the hotline itself does not issue "takedown" notices because in Spain only the court and other competent authority such as the police can issue such notices for taking down illegal content.

For the content hosted beyond the territory of Spain, the Protegeles hotline will keep the police of the concerned country informed through the Spanish police via Interpol or through its own contact point with law enforcement agencies in other jurisdictions.

For example, the Protegeles hotline has established a lot of contacts with several Latin American countries, especially Mexico, Venezuela and Brazil. The INHOPE member hotline working in the country that hosted the potentially illegal content will also be notified while the Protegeles hotline is one of the members of INHOPE.

Besides dealing with reports from the public, the Protegeles hotline also proactively searches illegal internet content using the public reports as intelligence as well as launching educative and preventive campaigns for raising social awareness on online children protection.

2.4.1.3 Germany

Germany is a country that has strict laws on pornography. Child and juvenile pornography are extremely restricted by the German Criminal Code. In addition, comprehensive police units are deployed to investigate and prosecute child sexual abuse content offences as well as the establishment of several non-governmental hotlines for reporting such content.

German Legislation

The German Criminal Code criminalises child and juvenile pornography and distinguishes their liability. As far as ISPs' liability for child sexual abuse content is concerned, the German Telemedia Act 2007 (Telemediengesetz- the TMG 2007) that transposed the Directive on Electronic Commerce is the law to apply in which liability of ISPs differs depending on their roles.

- **The German Criminal Code**

Child and juvenile pornography is regulated under Section 184 of the German Criminal Code. According to Section 176 (1) of the German Criminal Code, a child is a person under 14 years of age, and a juvenile refers to a person under 18 years of age in Section 182 (1) of the same Code. Pornographic written materials relating to sexual abuse of children or juvenile[36] are defined as child or juvenile pornography which constitutes a crime. The term "written materials" includes audio and visual recording media, data storage media, illustrations and other depictions pursuant to Section 11 of the Criminal Code.

[36] See Section 184b of the Criminal Code.

In the Criminal Code, distribution, acquisition and possession of child and juvenile pornography are criminalised. Pursuant to Section 184b of the Criminal Code, it is a criminal offence subject to three months to five years imprisonment when someone

- disseminates child pornography;
- publicly displays child pornography, presents child pornography, or otherwise makes child pornography accessible; or
- produces, obtains, supplies, stocks, offers, announces, commends, or undertakes to import or export in order to use child pornographic materials or copies made from them or facilitates such use by another pornographic written materials related to sexual activities performed by, on or in the presence of children.

Similar activities relating to pornographic written materials concerning children between ages of 14 to 18 years are also punishable by imprisonment of not more than three years or a fine according to Section 184c of the Criminal Code.

- **The Implementation of the Directive on Electronic Commerce in Germany**

Germany was the first European country that had overall legislation regulating ISP liability for all internet related contents. Two laws - the Media Services State Treaty 1997 (Mediendienstestaatsvertrag - MDStV)[37] and the Federal Teleservices Act 1997 (Teledienstegestz - TDG)[38] were passed in 1997 at both Federal and State level in addressing ISP liability on the internet. Because Section 5 of the TDG mirrored Section 1 of the MDStV, provisions with regard to liability for ISPs were identical in these two statutes. The TDG 1997 was revised once in 2001 to implement the Electronic Commerce Directive and the provisions in relation to ISP liability for online content in this 2001 version of the TDG were later transposed into the TMG 2007 in an effort to unify regulations embedded respectively in three statutes[39].

Section 3 of the TDG 1997 distinguished three types of service providers: information providers, access providers and hosting service providers. Section 5 of the TDG 1997

[37] The Media Services State Treaty 1997 (Mediendienstestaatsvertrag - MDStV), (1997, July 13), available at http://www.kuner.com/ (English Version) (last visited January 2 2011)
[38] The Federal Teleservices Act 1997 (Teledienstegestz - TDG), (1997, July 22), available at http://www.iuscomp.org/gla/statutes/TDG.htm#5 (English Version) (last visited January 2 2011) (The Federal Teleservices Act 1997 was part of the Information and Communications Services Act and entered into force in Germany on 1 August 1997. It dealt *inter alia* with the liability of online service providers. The Telemedia Act 2007 (Telemediengesetz-TMG) has now replaced it.)
[39] Here it refers to the Federal Teleservices Act 1997 (Teledienstegestz-TDG), the Teleservices Data Protection Act 1997 (Gesetz über den Datenschutz bei Telediensten) and the Media Services State Treaty 1997 ((Mediendienstestaatsvertrag-MDStV)).

then provided limitation of liability for those service providers[40] and their duty to block the use of illegal content[41]. The revised TDG 2001 that implemented the Directive on Electronic Commerce strongly reflected the Directive on Electronic Commerce and took over many aspects of the Electronic Commerce Directive. In particular, it implemented liability limitation of the Directive for ISP's activities as a mere conduit, caching and hosting and those provisions in the TDG 2001 were transposed into the TMG 2007 where the content of limitations of liability for ISPs was not changed[42]. Among other things, hosting ISPs are specifically required by Section 10 of the TMG 2007 (Section 11 of the TDG 2001)[43] to prevent public access to illegal internet content on their servers, expeditiously remove (takedown) or disable access to (blocking) the information after obtaining knowledge about such content. Nevertheless, blocking access to child sexual abuse content on access provider level[44] is being prevented when the current German government (in power since September 2009) has agreed to pursue the "deletion instead of blocking" ("Löschen statt Sperren") approach.[45] Therefore, the implication of the transposition of the Directive on Electronic Commerce into the German law on child sexual abuse content is that, a service provider which hosts child sexual abuse content material has no responsibility for the material on the condition that they remove or prevent access to the material immediately after acquiring knowledge about such content.

Despite the German law setting out ISPs' obligation for taking down illegal internet content, a "notice and takedown" procedure is not provided. Thus, the law offers little by way of practical advice to the public or right holders on how to send a notice to inform ISPs of unlawful content, or to ISPs on how to make decisions on requests for takedown. Nevertheless, voluntary Codes of Conduct have been developed to help

[40] Section 5 of the TDG 1997: (1) Service providers are responsible under the general laws for their own content which they make available for use. (2) Service providers are only responsible for third party content which they make available for use if they have knowledge of such content and blocking its use is both technically possible and can be reasonably expected. (3) Service providers are not responsible for third-party content to which they merely provide access for use. The automatic and temporary storage of third-party content because of a user access constitutes the provision of access.
[41] Section 5 (4) of the TDG 1997: Any duties to block the use of illegal content according to the general laws remains unaffected, insofar as the service provider gains knowledge of such content while complying with the obligation of telecommunications secrecy under Section 85 of the Telecommunications Law, and blocking is both technically possible and can be reasonably expected.
[42] Limitations for liability was in Section 8 to 11 of the TDG 2001 and they are currently in Section 7 to 10 of the TMG 2007 where limitation of liability for content providers is given by Section 7 (1) of the TMG 2007, limitation for liability of access providers is given by Section 8 & 9 of the TMG 2007 and limitation of liability for hosting service providers is regulated by Section 10 of the TMG 2007.
[43] Section 10 of the TMG 2007 (Section 11 of the TDG 2001): [P]roviders shall not be responsible for third party information that they store for a user if,
1. they have no actual knowledge of illegal activity or information and, as regards claims for damages, are not aware of facts or circumstances from which the illegal activity or information is apparent, or
2. act expeditiously to remove or to disable access to the information as soon as they become aware of such circumstances. Sentence 1 shall not be applied if the user is subordinate to or supervised by the provider.
[44] Section 9 (1) – (2) & 10 of the TDG 2001 (Section 8 & 9 of the TMG 2007) that corresponded to Article 12 (1) – (2) and 13 (1) of the Directive on Electronic Commerce address liability of access provider.
[45] See eco's response to question 26 of the IWF questionnaire.

ISPs monitoring the application of the legislation on the internet and, when possible, to report unlawful contents, identify their source and take down the content. With the establishment of self-regulation mechanism, the "notice and takedown" procedure has actually been activated in Germany.

Regulatory Regime in Germany

In Germany, there are two levels of police intervention against child sexual abuse content over the internet - German Federal Police (Bundeskriminalamt -BKA) and the State Police (Landeskriminalamt – LKA). When child sexual abuse content is reported to the police, action will be taken by the competent police body depending on the location of the content. In addition, there are three INHOPE member hotlines that provide the public channels for reporting child sexual abuse content, which are eco, FSM, and Jugendschutz. Since September 2007, the Federal Police (BKA) has signed a formal MoU with all three hotlines and agreed the hotlines to receive and pre-assess reports concerning child sexual abuse content.

Eco is the first non–governmental organisation that operates a hotline for the public to report illegal and harmful content posted online in Germany. It works in partnership with more than 500 members, among them the biggest host providers in Germany as well as the INHOPE member hotlines. To deal with the public's complaints concerning child sexual abuse content located in Germany, the eco content analyst will assess the illegality of the reported content first and then inform the appropriate police authority and notify the hosting ISPs after reporting it to the police (following a recent request of the BKA within their draft of the new MoU). For complaints concerning child sexual abuse content that is not hosted on a server in Germany, the hotline will send the reports to the respective countries with INHOPE member hotlines. If there is no INHOPE member hotline, the reports are brought to the attention of the BKA, which forwards the information via Interpol to the responsible police unit in the hosting country. The attention will be brought to the foreign hosting ISPs by the hotline as well.

Another hotline operated in Germany is FSM - an organisation for the voluntary self-control of the internet. The FSM hotline also deals with reports on illegal or harmful internet content. The public can report, *inter alia*, child sexual abuse content to the Complaint Office of the FSM and their complaints will be checked for possible violations of the German Criminal Code and will then be forwarded to the competent police unit. Takedown notices will be issued to domestic ISPs that hosted the

reported content. Information about internationally-hosted content will then be passed to INHOPE.

Similar to the hotline operated by eco and FSM, Jugendschutz runs a hotline that receives complaints that the public consider to be illegal or harmful to minors, including child sexual abuse content. A similar procedure run by eco and FSM is followed by the Jugendschutz for dealing with child sexual abuse content. The Jugendschutz works in co-operation with the INHOPE and other INHOPE member hotlines around the globe.

2.4.2 Countries in North and Latin America: the U.S., Brazil

2.4.2.1 The U.S.

In the U.S., there are two levels (federal and state) of laws dealing with child sexual abuse content and the laws have been developed to respond to the challenges presented by the internet and digital technology. Regulatory regimes relating to child sexual abuse content are also in place to facilitate investigation and prosecution of child sexual abuse content offences, including specific law enforcement agency and a hotline (CyberTipline) mandated by the federal law that assists law enforcement agency and Electronic Service Providers (ESPs) to eradicate online dissemination of child sexual abuse content.

The U.S. Legislation

In the U.S., the core Federal law regulating child sexual abuse related offences is the U.S. Federal Code. All 51 states of the U.S. also have their own laws in place for offences related to child sexual abuse content. For reasons of brevity, only the U.S. Federal Code is examined.

- **Provisions of the U.S. Federal Code Pertaining to Child Pornography Related Offences**

The U.S. Federal Code as amended by both the Child Pornography Prevention Act 1996 and the Protection Act 2003 prohibits the production, receipt, distribution, possession, transportation, mailing and advertising of any "visual depiction" involving the use of a minor.

A "minor" is defined as a person under the age of 18 by 18 U.S.C. §2256 (1) and the term of "child pornography" is defined by 18 U.S.C. §2256 (8) as:

> any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made

> or produced by electronic, mechanical, or other means, of sexually explicit conduct, where (A) the production of the visual depiction involves the use of a minor engaging in sexually explicit conduct; or (B) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

For the purpose of enforcing the federal law, 18 U.S.C. §2256 (2) defines sexually explicit conduct as actual or simulated sexual intercourse (including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, or lascivious exhibition of the genitals or pubic area of any person. A different definition of sexually explicit conduct within the context of computer-generated images is given by 18 U.S.C. §2256 (2) (B).

Production of child sexual abuse content including producing, directing, manufacturing, issuing, publishing or advertising (18 U.S.C. §2256 (3)) are further criminalized by 18 USC § 2251, which carries minimum fifteen years to maximum thirty years imprisonment, whereas possession, distribution and receipt of child sexual abuse content are criminalized by 18 USC § 2252 and 2252A, for which would be imposed minimum five years to maximum twenty years imprisonment for distribution or receipt of child sexual abuse content.

In addition, pursuant to 18 U.S.C. §1466A, it is a criminal offence to knowingly produce, distribute, receive, or possess with intent to distribute, a visual depiction of any kind, including a drawing, cartoon, sculpture or painting, that (1) depicts a minor engaging in sexually explicit conduct and is obscene, or (2) depicts an image that is, or appears to be, of a minor engaging in graphic bestiality, sadistic or masochistic abuse, or sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex and such depiction lacks serious literary, artistic, political, or scientific value.

According to 18 U.S.C. 2260, it is a felony for any person outside U.S. territory to produce or traffic in child sexual abuse content with the intent that the materials be imported into the U.S.. This provisions is an extraterritorial application of U.S. law to non - U.S. citizens.

- **Provision of the U.S. Federal Code Pertaining to Reporting Obligation of ESPs**

Under 18 U.S.C. § 2258A, legal responsibility of ESPs for reporting child sexual abuse content is provided. This provision introduces a "duty to report" when an electronic communication service or a remote computing service has "knowledge of facts or circumstances from which there is an apparent violation of section 2251, 2251A, 2252, 2252A, 2252B, or 2260 that involves child sexual abuse content; or section 1466A"[46]. The provision requires ESPs to register with CyberTipline – a hotline at the NCMEC to report crimes against children including child sexual abuse content, and, as soon as reasonably possible, to make a report of such facts or circumstances to the CyberTipline. The facts and circumstances included in each report may include information about the involved individual, historical reference, geographic location information, images of apparent child sexual abuse, and complete communication. The CyberTipline will then forward the report to a law enforcement agency or agencies designated by the Attorney General for investigation and/or possible prosecution. If an ESP knowingly and wilfully fails to make a report, a fine up to $150,000 (approximate 97,433 GBP) will be imposed for an initial failure and a fine up to $300,000 (approximate 194,867 GBP) will be imposed for any subsequent failure.

Nevertheless, ESPs are not required by the law to actively monitor any user, subscriber, or customer of that provider and the content of any communication of any user, subscriber, or customer of the provider; or affirmatively seek facts or circumstances from which a violation of child sexual abuse content is apparent.

Under the provision, the responsibility of the Attorney General and the CyberTipline (the NCMEC) are outlined as well as conditions of disclosure information contained within report and preservation of the report and its contents.

Regulatory Regime in the U.S.

In the U.S., the Federal Bureau of Investigation (FBI), the Department of Homeland Security's Immigration and Customs Enforcement (ICE), the U.S. Postal Inspection Service (USPIS), the Internet Crimes against Children Task Forces (ICACs), the U.S. Secret Service (USSS), the U.S. Department of Justice's Child Exploitation and Obscenity Section (CEOS) are working together against child sexual abuse content. While the mission of these law enforcement bodies is investigating and prosecuting child sexual abuse content related offences, the NCMEC encourages a multi-faceted approach including notice and takedown procedure to identify and remove child

[46] 18 USCS § 2258A (a)(2).

sexual abuse content from the internet.[47] The CyberTipline (a part of the NCMEC) mandated by the Federal law offers a hotline for reporting crimes against children including, the possession, manufacture, and distribution of child sexual abuse content. The CyberTipline operates in partnership with domestic law enforcement bodies as well as other international law enforcement.

Any incidents reported to the CyberTipline online or by telephone will be reviewed and prioritised by the CyberTipline operators and then NCMEC's Exploited Children Division will analyze tips and conduct additional research. The CyberTipline will then forward the report to a law enforcement agency or agencies designated by the Attorney General, including to the members of the ICACs. Additionally, all information is accessible to the FBI, ICE, and the USPIS via a secure Web connection. For reports concerning illegal contents against children outside of the U.S., pertinent international, state, and local authorities and, when appropriate, to the ESPs will be contacted.

In addition, the CyberTipline provides a list of child sexual abuse content websites to ESPs who have signed a MoU with NCMEC, but this is a voluntary program and is not required by the law. Therefore, the specific use and implementation of the list varies by ESPs. Several of the ESPs who receive the list block access to the websites listed while others may remove any content they are inadvertently hosting.

2.4.2.2 Brazil

Although the regulatory regime relating to child sexual abuse content in Brazil is relatively new and the hotline operated by the SaferNet Brazil is not yet a member of INHOPE, Brazil has had legislation concerning child protection since 1990 and the Brazilian National Congress has also approved new legislation regarding child sexual abuse on the internet in November 2008. In addition, a regulatory regime relating to child sexual abuse content over the internet has been gradually established with full support of the law enforcement agencies and collaboration of the ISP industry.

Brazilian Legislation

Brazil has the Law No. 8069 of July 13, 1990 for protection of children and adolescents. The law was amended by Law No. 11 829, DE 25 NOVEMBER 2008 in which offences relating to child sexual abuse content over the internet are criminalised as well as ISPs' liability for such content.

[47] See ICMEC, "Resolution of the Board of Directors", 15 October 2010, available at http://www.icmec.org/en_X1/pdf/Blocking_Resolution_EN.pdf (last visited on 17 November 2010).

- **Law No. 8069 of July 13, 1990**

Law No. 8069 of July 13, 1990 is the law that provides for full protection to children and adolescents in Brazil. The law not only provided legal definition of a child, but also clearly stated the fundamental rights of children.

In Article 2 of the Law, a child is defined as a person under 12 years of age and an adolescent is a person between 12 and 18 years of age. No child or adolescent will be subject to any form of neglect, discrimination, exploitation, violence, cruelty and oppression, be punished as any violation of law, by act or omission, their fundamental rights, according to the law.

Production and publication of photographical materials involving children or adolescents are prohibited by Article 240 and 241 of the Law but these two Articles were later amended by Law No. 11 829, DE 25 NOVEMBER 2008 in order to accommodate new offences relating to child sexual abuse content over the internet.

- **Law No. 11 829, DE 25 NOVEMBER 2008**

Law No. 11 829, DE 25 NOVEMBER 2008[48] was passed to combat offences of child sexual abuse content facilitated by the internet and digital technology. In particular, the law amended provisions of Article 240 and 241 of Law No. 8069 of July 13, 1990 in relation to production, sale, distribution, acquisition, and possession of child sexual abuse content. Pursuant to Article 240 of Law No. 11 829, DE 25 NOVEMBER 2008, it is a criminal offence to produce, reproduce, direct, photograph, film or record, by any means, scene of explicit sex or pornography, involving children and adolescents. Imprisonment of four to eight years and a fine will be imposed on an offender who has committed the above-mentioned crime. Article 241 then stipulates criminal liability of selling or exposing photos, videos or other recordings that contains the scene of explicit sex or pornography involving children or adolescents and penalties for such activity. By provision of Article 241-A, the law criminalises the offering, exchanging, delivering, transmitting, distribution, publication, and dissemination of photos, videos, or recordings containing the scene of explicit sex or pornography involving children or adolescents, by any means including by computer or telematic system.

Under Article 241-B, acquisition, possession or storage of, by any means, photos, videos or other recordings that contain the scene of explicit sex or pornography involving children or adolescents are criminalised with the exception to those who

[48] Law No. 11 829, DE 25 NOVEMBER 2008, available at http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11829.htm (Brazilian Version)

acquired, possessed or stored such content for reporting, investigating or prosecuting the crime relating to such content in the course of their legal duties and kept the content confidential. Simulated child or adolescent pornography including photos, videos or any other form of visual representations is also prohibited by Article 241-C as well as activities of selling, offering for sale, offering, distributing, publishing or disseminating, by any means, simulated child or adolescent pornography.

Under § 2 of Article 241-A, legal liability of ISPs is provided where the law explicitly states that imprisonment from three to six years and a fine will apply to a person who provides service or facilitates the storage of photos, pictures or images that contain the scene of explicit sex or pornography involving children or adolescents but fails to disable access to the content after being officially notified the existence of such content.

For the purpose of enforcing the law, definition of the term "sex scene explicit or pornographic" is given by Section 241-E – a provision that is in line with Article 2 (c) of the 2000 United Nations Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution, Child Pornography to which Brazil is a signatory since 2004. Therefore, in Brazil, child sexual abuse content refers to "any situation involving children or adolescents in explicit sexual activities, real or simulated, or exhibition of the genitals of a child or teen for primarily sexual."

Regulatory Regime in Brazil

In Brazil, law enforcements agencies such as Brazilian Federal Police (the Brazilian Federal Police Cybercrime Unit and the Brazilian Federal Police Child Sexual Abuse and Hate Crimes Unit) and Federal and States Prosecution Officer are the legal regulatory body for investigation and prosecution of child sexual abuse content related crimes. In addition, Brazilian National Cybercrime Reporting Centre was established in 2006 and is now operated by the SaferNet Brazil for reports concerning human rights cyber crimes and violations in the country, including reports regarding child sexual abuse content.

The SaferNet Brazil is a non-governmental organization established in December 2005 to protect, *inter alia*, children online. Since 2006 the SaferNet Brazil operated the Brazillian National Reporting Centre for Cybercrimes against Human Rights. To help receive and trace reports from the public, to produce official figures regarding cybercrimes against human rights, and to promote awareness and education campaigns in Brazil, SaferNet Brazil signed more than 30 formal co-operation

agreements with several major ISPs such as Microsoft, MySpace, Google and the main public and private institutions relating to child protection in Brazil, including

- Brazilian Federal Prosecutor Service in Sao Paulo, Rio de Janeiro, Rio Grande do Sul, Goiás, Paraná and Paraíba,
- Brazilian National Council of States Prosecutors General,
- Brazilian Internet Steering Committee,
- Brazilian Chamber of Deputies,
- Brazilian Federal Police,
- Brazilian Federal Senate,
- Brazilian Human Rights Secretariat at the President of the Republic Office,
- Brazilian Telecommunications Operators Association,
- Brazilian Mobile Phone Operators Association,
- Brazilian Credit Cards and Banks Association

Since November 2008, the SaferNet Brazil has a formal mandate to centralize all reports from Federal Police, Federal Government and Prosecutors Offices regarding human rights cyber crimes and violations in the country, including reports concerning child sexual abuse content.[49] The SaferNet Brazil hotline is required, under the provisions of the MoUs with the law enforcement bodies[50], to notify the corresponding authorities of any occurrences of child sexual abuse content being reported in order to enable necessary investigations and further actions. In addition, the competent law enforcement body has unrestricted access to the SaferNet Brazil database.

For the purpose of reporting child sexual abuse content on websites and social networks sites, the SaferNet Brazil Hotline signed the MoUs with Telecom/Mobile operators such as Telecom Italia Mobile, Brazil Telecom, Telefonica and internet content providers such as Google, MySpace, etc. The MoUs allow the SaferNet Brazil hotline to contact the Telecom/Mobile operators and ISPs regarding information concerning child sexual abuse content distributed within Brazilian internet territory and on relevant websites involving Brazilian users. In addition, the MoUs require the Telecom/Mobile operators and the ISPs to review and immediately forward to the SaferNet Brazil any reports of child sexual abuse content, together with other specific information, under the terms of a protocol mutually agreed upon.

[49] See Fabiana Frayssinet, "War Against Child Pornography on the Internet", available at http://ipsnews.net/news.asp?idnews=44906 (last visited on 18 July 2010)
[50] See http://www.safernet.org.br/site/institucional/parcerias/mpf and the MoUs being linked to.

Regular meetings between the SaferNet Brazil hotline and these involved parties are also established in order to discuss issues relating to the implementation of the process and continuity of the measures provided for in their agreements, e.g. issues concerning exchange of information in relation to child sexual abuse content, or issues concerning development of tools that enable automation of receiving and managing reports and crosschecking a daily URLs list detected from reports sent by the public. The ISPs are further required to preserve the content published by users of social networks for a certain period of time, or data necessary for police investigations for a minimum of six months or so, and provide such data to the corresponding officials, upon court authorizations. A comprehensive and formal reporting procedure is therefore established for the co-operation between the SaferNet Brazil hotline and the relevant parties, in particular, for matters concerning time frame for the notified content being taken down, data retention and sharing of a updated URLs list associated with child sexual abuse content, etc.

Hence, for child sexual abuse content hosted within Brazilian internet territory or hosted by international ISPs that have offices or legal representative in Brazil, e.g. Google, Yahoo!, Microsoft, etc, reports will be forwarded to the appropriate ISPs and competent law enforcement agency by the SaferNet Brazil Hotline and the content will be taken down usually in no more than 24 hours by the ISPs and/or be investigated by relevant law enforcement bodies. However, for such content hosted beyond the Brazilian jurisdiction, information will be passed onto the hotline where the content is hosted and/or the SaferNet Brazil Hotline will contact the appropriate Interpol representative in Brazil or law enforcements agencies in other countries, such as FBI, ICE in the U.S. and CEOP in the UK.

Nevertheless, unlike the UK IWF and hotlines in Spain and Germany, the SaferNet Brazil Hotline does not provide and maintain a blacklist for content blocking as there are no blocking policies or initiatives in Brazil so far.

2.4.3 Asian-Pacific Countries: Australia, Taiwan, and Thailand

2.4.3.1 Australia

In Australia, child pornography and child abuse related offences are prohibited by the laws both at Commonwealth (Federal) and State/Territory level. For eliminating the dissemination of child pornography or child abuse content over the internet, provisions of Commonwealth's Criminal Code (as amended) create ISPs' reporting obligation and that of the Broadcasting Services Act 1992 (as amended) then provide penalty for ISPs' failure to promptly take down child pornography or child abuse

content. A mandated notice and takedown procedure has been put in place for the eradication of child pornography or child abuse content over the internet.

Australian Legislation

In Australia, there are both the Commonwealth (Federal) and State/Territory laws that criminalise child pornography or child abuse related offences including possession, production, and sale/distribution of child pornography or child abuse materials (which covers the publication or making available of child pornography or child abuse materials). The States and Territories are generally responsible for the enactment of child sex-related offences, including child pornography offences, but provisions relating to such offences differ between the various states, in terms of formulation of the offences and the penalties. The Commonwealth has also enacted child sex-related offences, including child pornography offences, directed at conducts occurring across jurisdictions, e.g. where the internet is involved. For reasons of brevity, only legislation at the Commonwealth (Federal) level is discussed in this report.

- **The Commonwealth's Criminal Code (as Amended)**

In Section 473.1 of the Commonwealth's Criminal Code, "child pornography material" is defined to cover a range of material including that which depicts or describes a person under 18 engaged or involved in a sexual pose or sexual activity and material the dominant characteristic of which depicts for a sexual purpose the sexual organs, the anal region, or the breasts of a person under 18. Section 473.1 also defines "child abuse material" as material that depicts or describes a person under 18 as a victim of torture, cruelty, or physical abuse and does so in a way that reasonable persons would regard as being, in all the circumstances, offensive. However, a child is defined as a person under 18 years of age under schedule 7 to the Broadcasting Service Act 1992.

As for child pornography related offences involving the use of the internet, Sections 474.19 and 474.22 of the Commonwealth's Criminal Code Act 1995 (as amended) make it an offence to use a carriage service (e.g. the internet or mobile phone) to access, cause to be transmitted, transmit, make available, publish or otherwise distribute child pornography or child abuse material. In addition, Sections 474.20 and 474.23 make it an offence to possess, control, produce, supply, or obtain child pornography or child abuse material for use via a carriage service. The maximum

penalty for all Commonwealth child pornography and child abuse material offences is fifteen years imprisonment.

ISPs' liability for child pornography or child abuse material is then regulated by Section 474.25 according to which internet service providers or internet content hosts are obliged to refer details of child pornography or child abuse material to the Australian Federal Police within a reasonable time if they are aware that they are hosting child sexual abuse material.

- **The Broadcasting Services Act 1992 (As Amended)**

Apart from the penalties for internet service providers and internet content hosts who do not report child pornography sites to the police within a reasonable period of time, Schedule 5 to the Broadcasting Services Act 1992 (as amended) provides for the development and operation of industry codes of practice for the internet industry, and requires internet service providers and internet content hosts to inform users about content filtering tools. Schedule 7 to the Broadcasting Service Act 1992 (as amended) also sets out procedures relating to the takedown of prohibited content, including child abuse material that is refused classification and provides serious penalties for an ISP that fails to comply with a takedown notice issued by the Australian Communications and Media Authority (the ACMA).

Under the authorization of the Broadcasting Service Act 1992 (as amended), if the ACMA is satisfied that content is prohibited, having been refused classification by the Classification Board (under the National Classification Scheme), and the hosting service has an Australian connection, the ACMA may give a hosting service provider a notice directing the provider to remove the potential prohibited content. The hosting service provider must comply with the notice (an interim takedown notice, or a final takedown notice, or a special takedown notice) that applies to the provider as soon as practicable, and in any event by 6pm on the next business day, after the notice was given to the provider, pursuant to 53 of Schedules 7 to the Broadcasting Service Act 1992 (as amended). If the ISP fails to comply, they may commit an offence under clause 106(1) of Schedules 7 and may be imposed penalties of up to 100 penalty units (being Australian Dollar 11, 000, which is approximate 5,801 GBP) per day, or may in the making of a civil penalty order by the Federal Court (under clause 107 of Schedules 7) if the designated content/hosting service provider contravenes a civil penalty provision.

For the purpose of assessing whether the content is prohibited, National Classification Scheme also applies in which identical definition for child pornography or child abuse material is given as that in the criminal legislation. According to the Refused Classification category (RC) of Guidelines for the Classification of Films and Computer Games, materials that contain "descriptions or depictions of child sexual abuse or any other exploitative or offensive and descriptions or depictions involving a person who is, or appears to be, a child under 18 years" are refused classification and are therefore prohibited.

Regulatory Regime in Australia

Apart from the Australian Federal Police and/or the police force of a State or Territory that investigate internet child pornography or child abuse material related offences, the ACMA is another statutory authority established under the Australian Communications and Media Authority Act 2004 for regulating internet content including child pornography or child abuse content.

Since July 2000, the ACMA has administered a co-regulatory scheme for protecting children from exposure to unsuitable online content and to restrict access to certain internet content against children. The co-regulatory scheme is implemented through codes of practice developed by the internet industry, which are registered under the Broadcasting Service Act. Under the mandate of the Broadcasting Service Act 1992 (as amended), when the ACMA identified prohibited internet content that is hosted in Australia, they must give the hosting provider a written interim takedown notice directing the provider to remove the potential prohibited content. The ACMA must also apply to the Classification Board under Clause 22 of the Act for classification of the content. When and/or if the material has already been classified by the Classification Board, the ACMA must issue a final takedown notice. Under the provisions of the Broadcasting Service Act 1992 (as amended), the ACMA must defer taking action in relation to child sexual abuse material in order to avoid prejudicing criminal investigations. The ACMA will only issue a takedown notice after confirmation from the police that doing so will not impact on a criminal investigation. The ISP must comply with the ACMA's requests by 6pm the following day or face serious penalties.

All overseas hosted child abuse material will be referred to the appropriate INHOPE member via the INHOPE database. Where content is found to be hosted in a country that does not have an INHOPE hotline, the ACMA refers the content to the Australian Federal Police, who liaises with international law enforcement agencies.

For child pornography or child abuse content hosted beyond the Australian jurisdiction and is prohibited or it is likely to be prohibited, after referring the content to the Australian Federal Police or the appropriate INHOPE hotline, the ACMA will refer the content to the accredited filter software providers to block the content concerned. A registered code of practice for Australian ISPs requires them to provide a filter software product "at cost" to their customers, for the purpose of blocking such content.

Under the Broadcasting Services Act 1992 (as amended), the ACMA hotline must refer child sexual abuse content hosted in Australia to the relevant State or Territory police in order to facilitate investigation of related offences and effectively tackle child pornography and child abuse content over the internet. Further to this, a Memorandum of Understanding is in effect between the ACMA and Federal and State and Territory Police to facilitate sharing of information and assist criminal investigation.

2.4.3.2 Taiwan

There are several laws in Taiwan regulating child sexual abuse content and related criminal offences. Despite cases of child sexual abuse content related offences not being the primary concern of the law enforcement in Taiwan, a specific hotline - Internet Safety Hotline web547 is established working along with the Police hotline for reporting child sexual abuse content.

Legislation in Taiwan

In Taiwan, child sexual abuse content is defined by the Children and Youth Welfare Act and the Internet Content Rating Regulation. Activities relating to child sexual abuse content are criminalised by provisions of the Child and Youth Sexual Transaction Prevention Act and the Criminal Code.

- **The Child and Youth Welfare Law**

Despite the age of 18 being the age that has been used to decide whether a person should be treated as a child or an adult, [51] no explicit definition of a child is given in the law of Taiwan. It is said that the Child and Youth Welfare Law in 2003 broadened

[51] Article 18 of the Criminal Code of Taiwan distinguishes the criminal liability of a person under 18 years of age or over 18 years of age. In addition, the Child and Youth Welfare Law

its scope to include children under the age of 18 and thereby adhered to the definition of children in the Convention of United Nation[52] regarding children.

Article 30 of the Child and Youth Welfare Law stipulates that no one shall use children or young people to produce or film the publications, pictures, videotapes, films, compact discs, disks, electronic signals, games software, internet or other products with contents of violence, sexual passion, obscenity, gambling that are harmful to physical or mental health. Any products that are harmful to the physical and mental health of children and young people as recognized by the competent authorities shall be also classified, pursuant to Article 27 of the law. If the content is classified as restricted, the content should be labelled and access to it should be restricted by the ISPs. In the event that the content is deemed as against the law or the rules of the Internet Content Rating Regulation, by relevant government agencies or other commissioned bodies and an ISP has been informed of the unlawful content on its sever, the offending content should be removed.[53]

It is necessary to point out here that the criteria for assessing internet content are the Internet Content Rating Regulation – an administrative law passed based on Section 3, Article 27 of the Child and Youth Welfare Law, in which content that harms the physical or mental development of children or adolescents shall be rated as restricted under the provision of Article 4. In addition, Article 8 of the Internet Content Rating Regulation creates an obligation for internet service providers to restrict access to illegal or banned material or take them down if they have been notified by government agencies or other commissioned bodies of the existence of content on their network that are against the law or the rules of these Regulation.

- **The Child and Youth Sexual Transaction Prevention Act 1995 (as Amended 2007)**

The Child and Youth Sexual Transaction Prevention Act 1995 (as Amended 2007) provide criminal liability for certain activities relating to children under the age of 18. Under the provision of Article 27, it is unlawful for anyone to shoot or produce pictures, video tapes, films, CDs, electronic transmission or other products of sexual intercourse or obscenity of the person under the age of 18, otherwise, imprisonment from minimum of six months and up to maximum of five years and a fine shall be imposed. A higher penalty will be imposed on those who commit the crime prescribed with the purpose of making a profit. In addition, Article 28 criminalises activities of

[52] Here it refers to the 1989 United Nations Convention on the Rights of the Child.
[53] Internet content is classified according to the Internet Content Rating Regulation which was made in 2004 for classifying Internet content based on Section 3, Article 27 of the Children and Youth Welfare Act. Pursuant to Article 3 of the Regulation, Internet content shall not include illegal or banned material.

those who distribute, broadcast, or sell, film, produce photographs, movies, videos, DVDs, digital files, and other materials, display these materials in public, or use other methods to present them to others. Anyone who knowingly does that will be sentenced to maximum three years imprisonment and fined. For those who attempt to distribute, broadcast, sell, and possess the above items will be sentenced to maximum two years imprisonment and also be fined. Simple possession of the films and productions of child and teen photographs, movies, videos, DVDs, digital files, and other materials without proper reason will also be sentenced to two to ten hours rehabilitation under the local county (city) authorities, or will be subjected to a fine if a second offence occurs.

- **The Criminal Code**

The Criminal Code of Taiwan is also the law applicable to child sexual abuse content related offences but Article 235 criminalises such offences in a general term by stating that it is unlawful for a person to distribute, broadcast or sell material containing obscene language, or obscene pictures, sounds, images or other objects, or publicly displays or otherwise enables others to read, view or hear the same. Therefore, the law does not provide clear definition as to what constitutes obscenity and whether child sexual abuse content is considered as obscene material within the meaning of Article 235. Under the same provision, maximum two years imprisonment, detention and/or a fine shall be imposed on the person who commits the crime. The same penalty also applies to a person who manufactures or possesses the kind of material containing obscene language, pictures, sounds, images and the objects to which they are affixed or other matters with intent to distribute, broadcast or sell the same.

Regulatory Regime in Taiwan

Apart from the hotline operated by the Criminal Investigation Bureau of Taiwan for receiving all criminal reports from the public, the ECPAT Taiwan (Internet Safety Hotline web547) is the only non-governmental organisation that has a hotline for reporting child sexual abuse content in Taiwan. The Internet Safety Hotline web547 is also the member of INHOPE and ECPAT International (End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes)

Since its establishment in 1999, the Internet Safety Hotline web547 has been operated with similar processes as many other hotlines. When reports concerning illegal and harmful internet content including child sexual abuse content are received

by the hotline, the hotline staff will determine whether the content concerned is potentially illegal or inappropriate as well as trace the origin of the content. If the child sexual abuse content is hosted in Taiwan, the Internet Safety Hotline web547 will inform the 9th investigation brigade of CIB in Taiwan before issuing notices to the concerned ISP for taking down so that the Police can collect evidence and relevant information for possible criminal investigation. ISPs generally remove child sexual abuse content within 1-2 days after receiving notification from law enforcement or the Internet Safety Hotline web547.

For child sexual abuse content deemed potentially unlawful but hosted abroad, the Internet Safety Hotline web547 will forward the reports to INHOPE members or ECPAT members so that the reports can be transferred to the local law enforcement agency in the country concerned for further investigation and actions. Because the Taiwanese law enforcement agency is not a member of the Interpol, information concerning child sexual abuse content overseas cannot be passed onto the law enforcement body in the country concerned.

So far there is no blocking by ISPs in Taiwan and the Internet Safety Hotline web547 does not share a blacklist with ISPs for blocking potentially unlawful content hosted overseas. However, the Internet Safety Hotline web547 does provide a blacklist to the Ministry of Education Computer Centre in order to block sites and prevent children from accessing them while at schools (at elementary and junior high school levels.)

To date, the key part of the relationship between the Internet Safety Hotline web547 and the law enforcement body is the exchange of information, in particular, with regard to the reports concerning child sexual abuse content and the contact information of the police officers who are responsible for the relevant cases. The hotline has been working to maintain a good and close partnership with the law enforcement agencies in order to swiftly remove child sexual abuse content and facilitate investigation of child sexual abuse content related crimes in Taiwan.

2.4.3.3 Thailand

In Thailand, although no law specifically addresses child sexual abuse content, there are several laws dealing with pornography which are applicable to child sexual abuse content related offences. Several hotlines - either governmental or non-governmental – are operated in order to facilitate investigation and prosecution of child sexual abuse content related crimes and for the swift removal of such content.

Legislation in Thailand

Despite the facts that the 1989 UN Convention on the Rights of the Child and the 2000 UN Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography have been ratified by Thailand for years,[54] and that children under the age of 18 remain as the particular group safeguarded by the laws, Thailand does not have a specific law dealing with child sexual abuse content, only general provisions regarding pornographic and obscene materials are applied to child sexual abuse content related offences. As for child sexual abuse content over the internet, provisions of the Computer Crime Act B.E.2550 (2007) provide liability for individual offenders and ISPs that commit offences in relation to production, dissemination of any obscene computer data.

- **The Child Protection Act B.E. 2546 (2003)**

The aim of the Child Protection Act B.E. 2546 (2003) is to protect children from all forms of abuse, exploitation, violence and gross negligence. In this Act, a child is defined as a person below 18 years of age by Section 4. Chapter 2 of the Act is then designed specifically for treatment of the child. The provisions clearly state that children under the age of 18 are protected by the law and the State. In addition, the Act prohibits any person to force, threaten, use, induce, instigate, encourage, or allow a child to perform or act in a pornographic manner, regardless of whether the intention is for remuneration or anything else; and advertise by means of media or use any other means of information dissemination to disclose such pornographic pictures regardless of a child's consent.

- **The Penal Code Amendment Act (No. 14), B.E. 2540 (1997)**

Although the Penal Code Amendment Act (No. 14), B.E. 2540 (1997) does not specifically address child sexual abuse content related offences. Section 287 of the Act is a general provision applicable to both adult and child sexual abuse content in which any business involving the production, importing, exporting, distribution, selling, advertising or possessing obscene materials in any form is prohibited and is criminalised by the law with up to three years imprisonment and a fine.

- **The Computer Crime Act B.E.2550 (2007)**

[54] The 1989 UN Convention on the Rights of the Child was ratified by Thailand since 26 April 1992 and the 2000 UN Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography was ratified by Thailand since 11 January 2006.

As for liability for child sexual abuse content involving the use of the computer, the Computer Crime Act B.E.2550 (2007) is the main statute that aims to prevent and suppress the use of computer technology to disseminate pornographic computer data and criminalise such offences.

Section 14 (4) of the Act states that whoever inputs, into any computer system, any obscene computer data which is accessible to the public shall be punished with imprisonment up to five years and a fine. The same penalty will apply to activities of knowingly publishing and forwarding such obscene computer data according to Section 14 (5). Liability of service providers who intentionally support or consent to commit the offence under section 14 is then regulated by provisions of Section 15 of the Act with same punishment as prescribed in Section 14. Furthermore, Section 26 creates an obligation for ISPs to keep child sexual abuse content and data concerning the user of such sites stored for at least 90 days so as to facilitate investigation and prosecution by law enforcement agencies for child sexual abuse content related offences. ISPs may receive a fine if they fail to do so.

Regulatory Regime in Thailand

There are several hotlines operating in Thailand for receiving reports concerning child sexual abuse content, including the e-Cyber Crime Internet hotline staffed by the Royal Thai Police[55], a hotline of the Ministry of Information & Communication Technology[56] and a hotline run by the Ministry of Culture Thailand[57]. In addition, a reporting system is also developed by the Internet Foundation for the Development of Thailand with the operation of the Thaihotline, though the operation of this is at an early stage due to the fact that the hotline has only been operating for just a year from 2009 and needs to be further resourced and developed.

Similar to the models of several other hotlines such as the IWF, the Protegeles, and the German eco hotline, the Thaihotline is a non-governmental organization and receives funds from many sources such as ISPs, and the Thai Health Promotion foundation, etc. While keen to be working with other international hotlines in combating child sexual abuse content over the internet, the Thai hotline is not yet a member of the INHOPE but is currently in the process of applying for INHOPE membership.

[55] See http://ecybercrime.police.go.th/
[56] See http://www.mict.go.th/main.php?filename=index_complaint
[57] See http://www.m-culture.go.th/

Though the work of the Thaihotline is supported by the ISP industry, there is no formal agreement between the hotline and ISPs in terms of the co-operation in the field of removing child sexual abuse content. Therefore, the Thaihotline is now working on developing the MOU to improve the collaboration of self regulation between the hotline and ISPs. The Thaihotline only reports cases to ISPs for the consideration of removing, blocking or taking legal actions in each case concerning child sexual abuse content. But the action taken by ISPs depends on their priority and considerations of the cases as the ISPs are not obliged to take down or block any content, except upon authorization of a court order. Therefore, reactions to the notices of the Thaihotline vary, with some ISPs ignoring their reports but some taking actions against potentially unlawful content reported.

The relationship between the Thaihotline and the law enforcement agencies is also developing. So far there is no formal agreement signed between the Thaihotline and the law enforcement agencies, therefore the Thaihotline only transfers reports to the Police or the Ministry of Information & Communication Technology by sending email or report through their website. Though the Thaihotline provides the public with a channel for reporting potentially unlawful content and acts as a party for pre-assessing content reported, there is no further communication and exchange of information between the Thaihotline and the law enforcement agencies. Unlike other hotlines such as the IWF, the Protegeles that receive feedback from and have regular contact with the law enforcement agencies, the collaboration between the Thaihotline and the law enforcement agencies is far from optimal and needs to be strengthened.

2.5 Conclusion

It can be seen from the examination of the international and national laws of several countries that child sexual abuse content has been a serious concern around the globe and significant efforts have been put forward to eradicate online dissemination of child sexual abuse content.

International legal instruments provide a baseline international legal standard for the protection of children from sexual exploitation. Most countries have specific legislation or provisions on child sexual abuse content and ISPs' liability in relation to online child sexual abuse content, as is the case in the UK, Spain, Germany, the U.S., Brazil, Australia, and Taiwan. However, in the countries discussed above, only Thailand does not have specific legislation or provisions on child sexual abuse content related crimes, although general provisions on pornographic or obscene materials can still be applied in order to prosecute child sexual abuse content related offences.

Although a clear definition of "child sexual abuse content (child pornography)" is not provided in the legislation of all the jurisdictions other than that of Australia and the U.S., child sexual abuse content related offences such as, possession, production, distribution, and advertising of child sexual abuse content are prohibited by relevant laws and regulations in all the countries. As for ISPs' liability in relation to child sexual abuse content on the internet, all the countries have specific provisions in their law that set out the prerequisite for ISPs' liability and the consensus in their law is that an ISP that hosts child sexual abuse content has no responsibility for the material on the condition that the ISP removes, or prevents access to the content immediately after having the knowledge about such content. In both the U.S. and Australia, apart from statutory rules that criminalise activities relating to child sexual abuse content, there are also laws that assist the combating, e.g. requirements to report. Hence, ISPs in the U.S. and Australia have mandatory obligation to report child sexual abuse content hosted on their networks or face a heavy fine.

In addition, regulatory regimes regarding the effective removal of child sexual abuse content are also established in each country, with the UK, Spain, Germany, the U.S., and Australia having a more developed regulatory regime while the regulatory regime in Brazil, Taiwan, and Thailand is still at the stage of development. Specific law enforcement units/agencies have been established in each country for the investigation and prosecution of child sexual abuse content related crimes with the support of the public and relevant industries.

Apart from statutory regulation enforced by the law enforcement body and other competent state authorities, most countries have hotlines run by a non-governmental organisation for reporting child sexual abuse content, which effectively act as self-regulation body operated under industry Codes of Conduct. The hotlines inform the ISPs concerned about the occurrence of child sexual abuse content on their services and encourage them to take the content down in order to eradicate further dissemination of such content. In most countries domestic ISPs will usually take down child sexual abuse content after being notified by hotlines. In Spain and Thailand, ISPs are obliged to take down the content or block access to such content only upon the order of the court and/or other competent authority. For content hosted beyond the jurisdiction of one country, information regarding child sexual abuse content is transferred to the country concerned via the INHOPE network and the content is removed more quickly upon notices of the INHOPE members' hotline in the concerned country than through the Police and then Interpol.

The status of the hotlines differs between countries, with the hotlines such as the UK IWF, the Spanish Protegeles, the German hotlines, the SaferNet Brazil hotline, the Taiwan hotline, and the Thaihotline being non-governmental organisations. The hotlines of the U.S .and Australia are mandated by the law. All the hotlines other than the SaferNet Brazil hotline and the Thai hotline are members of INHOPE, which enable the hotlines to share data and expertise in order to better target resources and help inform and encourage international response to combating dissemination of child sexual abuse content across borders. In addition, at domestic level, many hotlines have established a closer partnership with local law enforcement agencies as is the case in the UK, Spain, Germany, the U.S., Australia, and Brazil, whereas in Taiwan and Thailand, such a partnership still needs to be strengthened.

Part 3: The Existing Regulatory Regimes relating to Child Sexual Abuse Content

3.1 Introduction

Regardless of the disparities between legal systems and legislations, law enforcement agencies in many countries have made significant progress in combating child sexual abuse related crimes through statutory regulation. Statutory regulation here therefore refers to a regulatory scheme established by law and enforced by law enforcement bodies, mainly by the police. Through reporting channels and other sources, national police forces are able to collect intelligence, track the source of child sexual abuse materials and offenders in order to investigate related criminal offences for possible prosecution. Nevertheless, the effectiveness of statutory regulation by the police force has been challenged due to the fact that, among other things, the process of police investigation for the crime is relatively long and cannot remove child sexual abuse content at source promptly and cannot therefore effectively prevent further dissemination of such content over the internet. For disrupting the availability and preventing dissemination of child sexual abuse content on the internet, self-regulation is encouraged in which a notice and takedown procedure and internet blocking is developed for removing or blocking such content. The notice and takedown procedure is proven to have had a beneficial effect in restricting the amount of child sexual abuse content hosted domestically and in limiting access to such content hosted abroad. internet blocking is also considered to have a role to play in reducing the risk of inadvertent exposure to online child sexual abuse content and in the reduction of re-victimisation of children.

It is incontrovertible that statutory regulation is essential for combating child sexual abuse content over the internet. Nevertheless, a self-regulation scheme can also work effectively due to the role which ISPs can play in the dissemination of child sexual abuse content. Hence, promotion of self-regulation measures should be given a high priority in constructing an effective regulatory regime concerning child sexual abuse content.

In this part, statutory regulation and self-regulation in the context of child sexual abuse content is discussed in order to give a comprehensive overview of strengths and weaknesses of the two regulatory schemes.

3.2 The Statutory Regulation Regime

Statutory regulation in this report refers to the regulatory scheme established by law and enforced by law enforcement bodies, mainly by the police. In this law enforcement approach, the police are authorised to investigate and prosecute child sexual abuse related offences in accordance with the specific law. For the purpose of statutory regulation in this regard, special units within the police force or police agencies have been established by a number of countries to deal with increasing child sexual abuse related crimes, as is the case in countries such as the UK, Spain, Brazil, the U.S., Australia, Canada, and Italy.

Statutory regulation is of paramount importance in identifying child sexual abuse offenders, protecting child victims, and prosecuting those suspected of child sexual abuse related crimes. However, it also shows a number of weaknesses, in particular with regard to the effective and timely removal of child sexual abuse content on the internet.

Since the relevant laws concerning child sexual abuse content have been discussed in Part 2 of the report, this part of discussion will focus on the law enforcement approach in respect of child sexual abuse content as well as its strengths and weaknesses.

3.2.1. The Strengths of Statutory Regulation

3.2.1.1 Establishment of Special Law Enforcement Agencies

In a number of jurisdictions, special units within the police force have been set up for combating child exploitation or child sexual abuse related crimes as the volume of child sexual abuse connected crimes have been increasing on the internet. According to the 2005 Report submitted by Mr. Juan Miguel Petit, Special Rapporteur on the Sale of Children, Child Prostitution and Child Pornography, special law enforcement units within the police force were established in eight different jurisdictions including Mexico, Croatia, Lithuanian, Luxembourg, Belgium, Switzerland, the U.S., and Norway by the end of 2004. Most of the special law enforcement units have a hotline and a web site to receive reports of cases of child sexual abuse content and other illegal activities on the internet.

Although the 2009 Report of the Special Rapporteur on the Sale of Children, Child Prostitution and Child Pornography did not provide updated data regarding special law enforcement units in other countries, more countries have, in fact, established special law enforcement units within their police forces for the investigation of child

sexual abuse offences. For instance, the Child Exploitation and Online Protection Centre (CEOP)[58] was established in the UK in 2006 working along with the local Child Abuse Investigation Units (CAIU) to protect children, investigate offences against children and, where appropriate, prosecute offenders. In Spain, the Technology Research Squad (previously known as the Information Technology Offences Research Squad) and the Guardia Civil Telematics Offences Squad were also formed for tackling child sexual abuse content and collaborating with special international unities such as Europol and Interpol for child sexual abuse content related crimes beyond the Spanish internet territory.

In Brazil, there are two special law enforcement units within the police for child sexual abuse related crimes - the Brazilian Federal Police Cybercrime Unit and the Brazilian Federal Police Child Sexual Abuse and Hate Crimes Unit. The Australian Federal Police Online Child Sex Exploitation Team (OCSET) is also a special law enforcement unit responsible for investigation and coordination within Australia for multi-jurisdictional and international online child sexual exploitation matters. According to the literature of Virtual Global Taskforce - "a global partnership that brings together national law enforcement agencies to protect children from sexual exploitation,"[59] Canada and Italy also have special law enforcement team established for crimes against children including child sexual abuse content related offences.

Despite the disparities between legal systems and legislations, special law enforcement agencies in different countries share the same goal, which is to investigate allegations of child abuse in accordance with their domestic laws in order to identify child sexual abuse offenders, to protect child victims, and, where appropriate, to prosecute child sexual abuse related offences in their territory.

For example, in the UK, the CAIUs and CEOP work together to investigate and prosecute child sexual abuse related offences when it comes to online protection of children. The local CAIUs take primary responsibility for investigating child abuse, with the variety of groupings of police officers from Specialist Paedophile Online Investigation Teams, Central Referral Units, Force Intelligence Bureaux, Child Protection, Teams, Public Protection Teams, High Tech Crime Units, Sexual Offences

[58] The Child Exploitation and Online Protection Centre (CEOP) is essentially a national law enforcement and child protection agency affiliated to the Serious Organised Crime Agency but retaining full operational independence. Before the establishment of CEOP, the UK government formed the Home Office Taskforce on Child Protection on the Internet in 2001 to bring together the Government, online technology providers, statutory and non-statutory bodies, law enforcement and child protection specialists for helping manage the risks arising specifically from the Internet. See UK House of Commons Culture, Media and Sport Committee, "Harmful Content on the Internet and in Video Games", Tenth Report of Session 2007–08, Volume I, Report, together with formal minutes, oral and written evidence, pp. 23-25.

[59] See Leaflet of the Virtual Global Taskforce, "About the VGT", available at http://www.virtualglobaltaskforce.com/pdfs/VGTLeaflet120308.pdf (last visited on 17 August 2010)

Units, Specialist Investigations Departments, or local Crime Investigation Departments. CEOP is the national centre dedicated to tackling sexual abuse and exploitation of children, having three faculties and a high volume of specialists. The responsibility of CEOP is, among other things, to gather and manage the flow of information concerning child abuse, to initiate harm reduction measures through education programmes for children and training for frontline professionals, and to support local police forces in areas such as computer forensics and covert investigations. In addition, CEOP works with international authorities to maximise policing powers.

When information about child sexual abuse content is reported to the CAIU, the CAIU staff analyse the information in consultation with intelligence officers and analysts in order to convert the information into intelligence. Through the application of the National Intelligence Model (NIM) and the strategic assessment process, the use of tactics that prevent further abuse and drive effective investigation are then decided.[60]

To assist the CAIUs investigation, in some cases, the CEOP will generate an intelligence package - the information received in the reports from members of the public and other sources - to provide further advice for investigation concerning child sexual abuse content in question. The intelligence packages allocated for investigations are likely to identify individuals who are suspected of child abuse content related crime. The activities of securing evidence of possession of such images, and identifying, locating and safeguarding any of the identifiable victims constitute the main task of the initial evidence recovery stage of the investigation. This initial evidence recovery stage will also assist in disclosing the role played by suspects in the production, possession and distribution of indecent images of children. Finally, the decision to arrest suspects may be made based on the analysis of the information.[61] In addition, CEOP also assists the CAIU on interviews and risk assessment of suspects through the work of its specialist operations and Behavioural Analysis Units.[62]

Special law enforcement agencies in other countries perform similar functions. For instance, in Australia, the Australian Federal Police Online Child Sex Exploitation Team (OCSET) plays an investigative and coordination role within Australia for multi-

[60] See the ACPO 2009 Guidance on Investigating Child Abuse and Safeguarding Children, "1.9.7 Use of the National Intelligence Model", p.59.
[61] See the ACPO 2009 Guidance on Investigating Child Abuse and Safeguarding Children, "4.3.3 Lines of Enquiry in Cases involving Child Abuse Images", p.124.
[62] See the ACPO 2009 Guidance on Investigating Child Abuse and Safeguarding Children, "4.10 Suspects Interviews", p.142.

jurisdictional and international online child sex exploitation matters. OCSET investigates online child sex exploitation and abuse offences involving the use of a telecommunications service (e.g. computers with internet connectivity or mobile phones), such as, offences of accessing, sending or uploading online child sex exploitation and abuse content as well as grooming and procurement of children on the internet.

In the U.S., when the public reports child sexual abuse content and other incidents of sexual exploitation of children to the CyberTipline operated by the NCMEC, NCMEC will refer the complaints that indicate a violation of federal law to the FBI for appropriate action. An FBI supervisory special agent and five analysts work full-time at NCMEC to assist with these complaints. The FBI analysts will then review and analyze the information received by the CyberTipline. Individuals suspected of child sexual abuse related offences, such as, possession, manufacture and/or distribution of child sexual abuse content will then be identified. Once a potential suspect has been identified, an investigative packet including the applicable CyberTipline reports, subpoena results, public records search results, the illegal images associated with the suspect and a myriad of other information will be compiled and forwarded to the appropriate FBI field office for investigation. For the investigation and prosecution of child sexual abuse content related crimes, the FBI also works in partnership with other law enforcement bodies such as the U.S. Department of Justice's Child Exploitation and Obscenity Section (CEOS) and the Internet Crimes against Children Task Forces (ICACs).

3.2.1.2 Progress Made by Special Law Enforcement Agencies

Special law enforcement units in a number of countries have made significant progress in the fight against internet child sexual abuse and exploitation. According to the UK CEOP Annual Review 2009-2010, the CEOP Centre received 6,291 intelligence reports between 1 March 2009 and 28 February 2010 – a culmination of reports through the public 'ClickCEOP' reporting mechanism, from the online and mobile industries and law enforcement partners in the UK and overseas. As the result of CEOP activity, either directly or indirectly, 278 children have been safeguarded or protected from sexual abuse between 1 April 2009 and 31 March 2010 while 47 of those have been identified through the victim identification process. During the same period, 417 suspected child sexual offenders have been arrested – for offences ranging from possession of indecent images to rape – as a result of intelligence reports from CEOP and/or through the deployment of CEOP resources. 96 high-risk

child sexual offender networks have also been disrupted or dismantled because of CEOP activity.

In the U.S., NCMEC received a total of 593,963 reports regarding child sexual abuse content possession, manufacture, distribution of child pornographic materials from March 9, 1998 through April 20, 2009. With the efforts of the NCMEC and enhanced law enforcement coordination, a total of 2,312 victims of child sexual abuse content crimes have been identified and many rescued, over 1000 of them since the launch of Project Safe Childhood in 2006 as of May 2009.[63] As for people being prosecuted for internet child sexual abuse content related cases, in 2008, 1,953 defendants were charged with federal internet child sexual abuse content related cases with 1,580 people pleading guilty only 5 of which were acquitted. In 2009, there is a slight increase in the number of defendants with 2,074 defendants being charged in 2009 and 1,769 of them pleading guilty for child sexual abuse content related offences.

Apart from the efforts by the domestic law enforcement agencies, there has also been international collaboration between law enforcement agencies of different countries that aims to tackle child sexual abuse related crimes across borders, such as, the international efforts made by Interpol and members of Virtual Global Taskforce.

As the world's largest police organization, the mission of Interpol is to assist law enforcement agencies in its 188 member countries to combat all forms of transnational crime. The unique position of Interpol in the international law enforcement community therefore gives it the resources and networks to fight online child sexual abuse related crime more effectively and in this role it acts as a central body to collect, store, analyse and disseminate information on child sexual abuse and child exploitation on the internet. Interpol manages the International Child Sexual Exploitation Image Database (ICSE DB) launched in March 2009. This ICSE DB replaced the Interpol Child Abuse Image Database (ICAID) that served investigators at the General Secretariat[64] for eight years and helped them to identify and rescue several hundred victims.

[63] The United States (January 22, 2010), "The Periodic Report of the United States to the United Nations Committee on the Rights of the Child and Response to Committee Recommendations", p.5.
[64] As outlined in the constitution of Interpol, the General Secretariat is responsible for carrying out the orders and decisions of the General Assembly and the Executive Committee. It serves as an international centre in the fight against crime and as an information and technical centre. It maintains contact with its member nations and their police authorities. It is located in Lyon, France and operates 24 hours a day, 365 days a year. See http://www.interpol.int/Public/icpo/ipsg/default.asp (last visited on 10 February 2011)

The ICSE DB contains more than 500,000 images of child sexual abuse and is available to certified investigators in any member country in order for them to analyze and share data with colleagues in other countries.[65] 1,453 child abuse victims had been identified and rescued worldwide by the end of 2009 based on the information of the ICSE DB.[66] In addition, Interpol has coordinated joint investigations against people who downloaded and distributed child abuse material worldwide, such as Operation Vico[67] and Operation IDent[68]. Furthermore, Interpol has co-ordinated the transfer of intelligence and/or evidential packages regarding child sexual abuse and child exploitation between countries so that intelligence and information can be shared in order to identify, locate and arrest child sex offenders around the world.

International collaboration is also achieved at practitioner level - the establishment of the Virtual Global Taskforce (VGT) is a good example. The VGT is an international alliance of law enforcement agencies dedicated to protecting children from sexual exploitation established in 2003. Member states and individual agencies of the VGT include the Australian Federal Police, the CEOP in the UK, the Italian Postal and Communication Police Service, the Royal Canadian Mounted Police, the US Department of Homeland Security, Interpol, the Ministry of Interior for the United Arab Emirates and New Zealand Police. The mission of the VGT is to make the internet a safer place; to identify, locate and help children at risk; and to hold predators appropriately to account. The VGT is intended to enhance existing law enforcement initiatives and intensify international relationships related to child exploitation issues. Members of the VGT have made substantial progress in facilitating cross country investigations and information sharing, for example, a successful 10-month investigation involving the co-ordination of law enforcement agencies from 35 different countries into a UK-based non-commercial online trading ground for indecent images of children and live exchanges of abuse in 2006-2007.[69] The VGT also launched Operation PIN in December 2003. Operation PIN was an operation involving the creation of a website that purports to contain images of child abuse but which, in fact, is a law enforcement site designed as a crime reduction initiative. The website was designed to capture the details of those who were actively looking for images of child sexual abuse from a number of different countries and to

[65] See Interpol Annual Report 2008, p.16
[66] See Interpol Annual Report 2009, p.5.
[67] See Interpol Annual Report 2008, p.25. (The first global public appeal for help in identifying a paedophile that led to the arrest in Thailand of Christopher Paul Neil in October 2007, now serving a prison sentence.)
[68] See Interpol Annual Report 2008, p.5. (An operation involving the Police in Norway, Canada, and the U.S. resulted in the identification and the arrest of a suspected child abuser in only 48 hours.)
[69] See Dr Victoria Baines (CEOP Principal Analyst, on behalf of the Virtual Global Taskforce), "Online Child Sexual Abuse: The Law Enforcement Response", November 2008, pp.15-16.

undermine the confidence of those who think that the internet is an anonymous place where paedophiles and other criminals can operate without fear of being caught. [70]

International collaboration between law enforcement agencies of different countries has also made contribution to combat child sexual abuse related crimes across borders. According to the annual report 2008/2009 of the Australian Federal Police, the High Tech Crime Operations team in Australia worked with the police of other countries as well as Interpol for the investigation of child sexual abuse. More than 150 people were arrested with downloading images of child sexual abuse and more than 15,000 videos and 500,000 images of child abuse were seized. 138 Australians were arrested in Operation Centurion as a result of a referral from the Croatian police via Interpol, whereas another 22 Australians were arrested during Operation Resistance as a result of a referral from the Brazilian authorities.

3.2.2 Inadequacy of the Law Enforcement Approaches

The examination above regarding the special law enforcement units in a number of countries and international collaboration as well as relevant statistics highlights the important work that the special law enforcement units and international partnership undertake in combating online child sexual abuse and child exploitation. The strengths of the law enforcement approaches are also identified in the discussion, in particular, the strengths in identifying child sexual abuse offenders, protecting vulnerable child victims, and where appropriate, prosecuting child sexual abuse related crimes. However, the data does not suggest the level of resources and the efforts of the law enforcement bodies are sufficient to tackle the threat posed by those who sexually abuse and exploit children at a significant level. As the CEOP Strategic Overview 2009-2010 accentuated that,

> What is universally agreed amongst law enforcement, however, is that the scale of abuse is potentially far bigger than that portrayed in the current picture and that there needs to be improvements in data collection in order to gain a much better understanding of the scale of child sexual abuse wherever it takes place.[71]

Although this statement was primarily intended to highlight the importance of the data collection concerning child sexual abuse content, it nevertheless reflected the scale of child sexual abuse content over the internet and the potential devastating

[70] See Virtual Global Taskforce, "What We Do", available at http://www.virtualglobaltaskforce.com/what_we_do.asp (last visited on 20 August 2010)
[71] See the CEOP Strategic Overview 2009-2010, p.9.

effect on child victim's reputation and emotional well-being. Dr Victoria Baines expressed the same view in her paper written on behalf of the ECPAT International: "[W]hat is clear is that the amount of identified traffic in child abuse material is greater than the law enforcement resources dedicated to investigate it."[72]

Even if the above observations are not representative, they do illustrate both the proliferation of child sexual abuse related crimes on the internet and the huge scope of the problem law enforcement agencies are facing. Discussions made earlier (see last paragraph of page 60 and first paragraph of page 61) indicate similar situation in the U.S. where it has been a steady increase on the numbers of child sexual abuse offenders, with 85% pleaded guilty in 2009 compared to 81% in 2008. In fact, there has been a proliferation of technology facilitated sexual abuse and exploitation crimes against children and a steadily increasing number of people being prosecuted and charged for federal internet child sexual abuse content related crimes in the U.S. since 1995,[73] despite extensive efforts of the law enforcement bodies.

Hence, the intensified law enforcement operations do not necessarily mean that such an approach is the most effective and sustainable approach to preventing child sexual abuse and child exploitation, in particular, to expeditiously removing child sexual abuse content at source.

To tackle the problem, apart from the law enforcement approaches implemented by the Police, other alternatives that can act more quickly to identify potentially illegal child sexual abuse content and remove them, where appropriate, should therefore be considered. These include commitment by ISPs and self-regulating bodies that can promote such a practice. Child sexual abuse content is a global issue, therefore, prevention of child sexual abuse content related offences and successful investigation of such a crime are only achievable through integrated partnerships between the law enforcement agencies and private sectors, non-governmental organisations and other stakeholders.[74] However, prior to the discussion of the self-regulatory model, it is necessary to examine the weaknesses of the law enforcement approaches that have an impact upon the effectiveness of the removal of child sexual abuse content in order to provide a better understanding of the crucial importance of self-regulation in the context of the expeditious removal of child sexual abuse content.

---

[72] See *supra* note 69, p.4.
[73] See Yaman Akdeniz, Internet Child Pornography and the Law, (Aldershot, England: Ashgate, 2008), p.131, Table 3.1 US child pornography prosecution and conviction statistics (1995-2006). Also see the United States (January 22, 2010), "The Periodic Report of the United States to the United Nations Committee on the Rights of the Child and Response to Committee Recommendations", pp.47-48. (The report provided a chart showing the increasing number of defendants charged in federal Internet child pornography-related cases from 2006 through 2009).
[74] *Ibid*, p.1

3.2.3 The Weaknesses of Statutory Regulation in Terms of the Swift Removal of Child Sexual Abuse Content at Source

It was pointed out in the 2005 Special Rapporteur Report of Mr. Juan Miguel Petit[75] that, although law enforcement operations have intensified in a number of countries following the establishment of special law enforcement agencies, the progress made has not been that great and the overall responses in place have not been adequate to the magnitude of the problem. The difficulties encountered by the Norwegian Criminal Police are an example of the problem. The Norwegian National Criminal Police had expressed their frustration and concerns about the effectiveness of statutory regulation, particularly in terms of investigation, intelligence and technological equipment to combat child sexual abuse content and abuse on the internet. They discovered that investigation of child sexual abuse related cases usually take several years before they reach the courts. A multitude of judges only have a limited understanding of electronic distribution methods and the extent of digital exchange of information about child sexual abuse content on the internet, which could again defer the cases and the effective removal of child sexual abuse content concerned. When the content has to be retained online for the investigation (for preserving evidence) and/or the removal can be only performed with the court order, the content would continue to circulate on the internet and would cause harm to the child victim's reputation and emotional well-being.

In the UK, it is also observed that, despite many efforts made by special law enforcement agencies for the investigation of child sexual abuse related crimes, "responsibility for investigations into online child sexual abuse remains fragmented."[76] The multiplicity of responsible investigative units in the UK can "present additional challenges to the successful coordination of investigations and strategies, and the development of skills and expertise,"[77] which may in turn affect the prosecution of child sexual abuse related crimes, let alone the effective removal of child sexual abuse content concerned.

This raises questions over the effectiveness and efficacy of the law enforcement approach (the more conventional police or court -based route), in particular, in terms of the expeditious removal of child sexual abuse content on the internet. The above studies suggest there is a contrast between the efforts taken by the law enforcement agencies to fight against child sexual abuse related crimes and the international proliferation of child sexual abuse content over the internet. Therefore, the

[75] See *supra* note 3, p.17.
[76] See *Supra* note 69, p.13.
[77] *ibid*.

weaknesses of the law enforcement approaches in terms of the expeditious removal of child sexual abuse content could be due in part to the following reasons:

- **The initiation of the investigation of child sexual abuse related offences does not necessarily mean that the child sexual abuse content concerned can be removed in the most timely manner.**

In some jurisdictions, child sexual abuse content identified may stay online for a certain period of time. For example, according to the Thaihotline, a process has to be followed in Thailand for the police to apply for a court order for requesting ISPs or ICPs to delete or block access to the content identified. Therefore, the deletion and blocking depends on the priority and/or consideration of the ISP or ICP. This indicates that child sexual abuse content reported to the ISP or ICP may remain online until the court/the police determine if the content would constitute a crime in their jurisdiction following the domestic laws and has to be removed or blocked. This is also the case in the U.S.. The U.S. federal law authorises the police to order an ISP, in the context of a criminal investigation, to keep a record of data about a specific person or IP address, pending issuances of the appropriate warrant requiring disclosure of that information.[78] Therefore, the reported child sexual abuse content may remain online longer in countries such as Thailand and the U.S. than that in the country, e.g. Australia. Because the Australian law authorises the statutory authority - the ACMA to issue a takedown notice directing that the Australian ISP must remove child sex abuse content by 6pm the following day after confirmation from the police, that doing so will not affect a criminal investigation. In some other countries, the content concerned may remain online even longer while ISPs are only obliged to take down content upon notifications of government agencies or other commissioned bodies and child sexual abuse related crime might not be the primary concern for law enforcement in the country[79] as is the case in Taiwan.

Hence, even if the child sexual abuse content has been reported to the police, the initiation of the criminal investigation may take quite some time and the ISP will only remove the content once the police order them to do so. As long as the content is available online, further circulation will be unavoidable and that would further harm the child victim's emotional well-being. For the content being preserved by ISPs under the requirement of the law, there is a potential that the content may be

[78] In the U.S., when ESPs report apparent child pornography in accordance with federal law, they are mandated to keep the content for 90 days. See 18 USC 2258A.
[79] See *supra* note 69, p.11 (Dr Victoria Baines cited Klain, Davies and Hicks's observation in 2001 that "child sexual exploitation is not a priority in many jurisdictions especially when competing for attention with street violence, gang activity, and drug trafficking" holds true seven years later, despite significant public interest in child protection and media attention afforded to this type of criminality: failure to include online child sexual abuse in government policing plans necessarily results in a lack of prioritisation and resourcing at both national and local levels.)

exposed to agents or employees of the ISPs if the content has not been properly maintained in a secure location and the ISPs did not take appropriate steps to limit access. In addition, the police investigation may have a different focus as they may concentrate more on prosecuting child sexual abuse offenders and protecting child victims rather than removing the content concerned at source and preventing its further dissemination.

Hence, even though information about child sexual abuse content may be quickly acquired by law enforcement agencies, such content may not be removed swiftly at source or taken down in order to avoid further dissemination or being stumbled across by the inadvertent users. The removal will depend on the priority of the law enforcement agency in a specific country and/or certain procedures established under relevant law.

- **A lengthy process is needed for criminal investigation and prosecution of the child sexual abuse related crimes, but, among other things, lack of resources (e.g. funding, expertise, and trained staff) may hinder the effective investigation and prosecution of the cases.**

Another factor that impedes the efficacy of the law enforcement approach in terms of the expeditious removal of child sexual abuse content on the internet could be that a significant length of time is required for investigating such cases involving rapidly expanding and evolving internet technology.

Child sexual abuse related offences are facilitated by advanced internet technology and child sexual abuse content can be disseminated quickly over the borderless internet. Therefore, investigation of child sexual abuse content tends to involve large numbers of criminal justice professionals who are trained with adequate knowledge about computer and internet technology, otherwise, the sheer size of the internet and the potential implications of investigating such a crime committed in a global arena can put law enforcement resources under considerable strain. Nevertheless, the resources and investigative capacity of the existing law enforcement agencies seems not to match the advancement of the technology and the scale of the problem. As Dr Victoria Baines observed,

> Law enforcement agencies in some nations have made significant progress in investigating the online sexual abuse of children and young people, most notably adopting a more victim-centred and collaborative approach. It must be acknowledged, however, that even those national specialist centres established since World Congress II are still insufficiently resourced to meet the challenges of investigating the sexual abuse of children and young people in an environment which is

constantly expanding and evolving, thereby providing unprecedented opportunities for sexual exploitation.[80]

For example, in Australia, lack of resource for investigating child sexual abuse related crime has been a serious concern. It was reported by the Daily Telegraph[81] that the Australian Federal Police agents had asked New South Wales Police to take over cases of paedophiles because they did not have the resources to investigate those cases. The Daily Telegraph revealed that an agent from the Australian Federal Police's online child sexual exploitation team had written to New South Wales Police on 7 November 2006 for help on a case involving a New South Wales man who had molested 100 children and groomed a 14 year old boy in the U.S. for sex on the internet. This matter was originally referred to an operational area of the Australian Federal Police but no investigational activity commenced at the time due to operational and resource issues. In addition, it was discovered that more than 100 child exploitation cases had also been handed to New South Wales Police in 2006 however only half were likely to be investigated. To enhance the specialised New South Wales child exploitation internet unit, the State Government had promised to recruit more staff (from 4 to 11 officers), but such a promise has not been delivered yet. The effect of failing to provide more resources has directly led to the loss of police officers in some of highly specialised information technology areas within the police, according to the Commissioner Ken Moroney of the New South Wales Police Force.[82]

The funding cuts by the Rudd government (2007-2010) could again affect the resources availability for police activities in Australia. The Rudd Government cut the allocation from $51.8 million provided by the Howard Government to enable growth in the online child sexual exploitation team to $49 million. The timeframe of the funding for the growth was also delayed from 2007 until 2010-2011. It remains to be seen if the work of the Australian Federal Police's online child sexual exploitation team will be prioritised under the current government's policy while some suggest[83] that it is vital "to increase the resources available to the AFP so that they are better able to investigate and arrest child abusers."

[80] See *supra* note 69, p.45.
[81] See Luke McIlveen, "No Money Available to Chase Internet Paedophiles", *The Daily Telegraph*, 18 June 2007.
[82] See "Report on Inquiry into the Future Impact of Serious and Organised Crime on Australian Society", Parliamentary Joint Committee on the Australian Crime Commission, 19 September 2007, paras 7.29.
[83] See Submission to the Australian Federal Parliament's Joint Select Committee on Cyber Safety by the Child Sexual Abuse Prevention Program, pp.4-5. Also see, Submission to the Australian Federal Parliament's Joint Select Committee on Cyber Safety by Mr. Mark Newton (an Internode's engineer at Internode - one of South Australia's largest regional ISPs), p8.

Therefore, to improve the efficacy of the law enforcement approach, it is imperative "to develop expertise and resources within national law enforcement agencies to ensure they have the right personnel and technology to allow them to act against child pornographers in their own countries, but also to participate in international actions against them."[84] Only by so doing will child sexual abuse related offenders be quickly identified and further circulation of child sexual abuse content prevented.

- **The global and borderless nature of online child sexual abuse related crimes makes investigations particularly difficult.**

The global and borderless nature of online child sexual abuse related crimes could be another factor impeding the efficacy of the law enforcement approach, in particular, in terms of the expeditious removal of child sexual abuse content on the internet.

Because the internet has no borders, child sexual abuse content can be easily made and uploaded in one country and be distributed to anyone in the world with merely a computer and an internet connection. According to the 2008 Annual Report of the Interpol, by the end of 2008, Interpol had images of more than 500,000 different children in the International Child Sexual Exploitation Database,[85] which does not include images held by national law enforcement agencies that have not been passed on to Interpol. The CEOP 2007-2008 Strategic Overview also suggests, "this year (2008) has also seen the emergence of images containing victims from atypical racial groups and in atypical locations, including South America and Asian countries such as South Korea, China and Japan. This proliferation of images from a variety of source countries may point to the role of the internet in facilitating truly global communications and networking across obvious language and cultural barriers."[86] Those numbers reflect that there has been and is a large number of child sexual abuse content available over the internet.

The fight against the production and distribution of child sexual abuse content is a challenge for law enforcement agencies, but differences between the laws and police systems make it more difficult to investigate and prosecute such internet facilitated crimes, as well as remove child sexual abuse content at source after criminal investigation and prosecution. Despite law enforcement agencies crossing all jurisdictions and collaborating internationally, the efficacy of the process, however,

[84] See *supra* note 69, p.11
[85] See Interpol Annual Report 2008, p.16
[86] See the CEOP 2007-2008 Strategic Overview, p.19

can be poor due to the slow and bureaucratic mutual legal assistance procedure.[87] With the assistance of Interpol, information sharing has been significantly improved, which has in turn facilitated more investigations. Nevertheless, differing law in countries can still create loopholes to allow child sexual abuse offenders to continuously distribute harmful content. For example, in the countries that did not criminalise the knowing possession of child sexual abuse content,[88] their law enforcement agencies may not seize such material and work to identify child victims appearing in those images or assist the investigations of other nations into online child sexual abuse, due to the lack of legislation against the possession of child sexual abuse content.

3.3 The Self-Regulation Regime

As mentioned in the previous discussion, an alternative that can act more quickly to identify potentially illegal child sexual abuse content and remove it, where appropriate, is self-regulation.[89]

Having discussed the strengths and weaknesses of statutory regulation in the context of the swift removal of child sexual abuse content on the internet, the report now examines the self-regulatory approach in eradicating illegal child sexual abuse content. By so doing, this part of the report makes a comparison as to whether the self-regulatory model is more efficient in terms of the expeditious removal of child sexual abuse content online.

3.3.1 Self-Regulation in the Context of Child Sexual Abuse Content

In the context of child sexual abuse content, self-regulation refers to the regulatory scheme developed by ISPs self-tailored technical mechanisms such as blocking or filtering for preventing child sexual abuse content and a notice and takedown system implemented by hotlines and ISPs for reporting and removing child sexual abuse content.

---

[87] See Ian Walden, "Porn, Pipes and the State: Censoring Internet Content", The Barrister, 13th April 2010, p.4. (Professor Ian Walden pointed out in this article that, the efficacy of the process can be poor for child sexual abuse content hosted aboard due to the fact that "mutual legal assistance procedures are notoriously slow and bureaucratic and, inevitably, the recipient state may not action the report for any number of reasons, from a lack of resource and conflicting priorities, to differences in the legal treatment of such content, such as age threshold (e.g. 16 or 18 years)."

[88] See *supra* note 31 (According to this study, 89 of 196 countries around the world had no legislation at all specifically addressing child pornography. Despite the 2007 Convention on Child Protection urges nations to criminalise possession, 33 of the countries that have legislation specifically addressing child pornography do not criminalise the knowing possession of child pornography, regardless of the intent to distribute).

[89] The discussion of self-regulation in this report does not necessarily mean the exclusion of other alternatives, e.g. co-regulation. Co-regulation would also be appropriate in certain circumstances. Discussion on co-regulation see *infra* note 151, p.251.

ISPs have a crucial role to play in the regulation of child sexual abuse content on the internet while they could be indirectly involved with the dissemination of child sexual abuse content. Self-regulation is considered as one of the ways for ISPs to exercise their control in stopping distribution of child sexual abuse content. Such control may not only take place at a national level, it may also be exerted on an International level by developing common standards and values and/or by establishing protocols to ensure child sexual abuse content hosted on one country's websites can be quickly reported to the authority of another country and can subsequently be removed.

In fact, self–regulation has been encouraged at both national and international levels. For example, in countries such as the U.S., Australia, and many European countries such as the UK, Germany, the Netherlands, Spain and Ireland, self–regulation is encouraged by the governments. In the context of child sexual abuse content, the set up of the hotlines for reporting online child sexual abuse content is particularly promoted. At an international regional level (e.g. Europe), the Safer Internet Programme - an initiative of the European Commission to fund activities to fight and prevent illegal and harmful content, as part of a coherent approach by the European Union, is a good example that self-regulation has been strongly encouraged within Europe. As a result, a European network of hotlines for reporting illegal content – INHOPE has been set up, with currently 29 hotlines in 25 European Member States.

With the support of the governments and international organisations, self-regulation initiatives are now more and more common in the context of combating child sexual abuse content. In the UK, the strengths of self-regulation is recognised in the Tenth Report of the Select Committee on Culture, Media and Sport[90] in which the report highlighted that "a self-regulating industry is better placed to respond quickly to new services; it is more likely to secure "buy in" to principles; and it will bear the immediate cost." By acknowledging significant progress has been achieved through self-regulation by the various industries offering internet-based services, the reports also pointed out that, "there appears to be a lack of consistency and transparency of practice, and the public needs the assurance that certain basic standards will be met." The report therefore suggested that, "[R]ather than leap to statutory regulation, we propose a tighter form of self-regulation, under which the industry would speedily establish a self-regulatory body to draw up agreed minimum

[90] See House of Commons, Session 2007-08, Publications on the internet Culture, Media and Sport Committee Publications, Culture, Media and Sport - Tenth Report, available at http://www.publications.parliament.uk/pa/cm200708/cmselect/cmcumeds/353/35302.htm (last visited on 16th September 2010).

standards based upon the recommendations of the UK Council for Child Internet Safety (UCCIS), monitor their effectiveness, publish performance statistics, and adjudicate on complaints. In time, the new body might also take on the task of setting rules governing practice in other areas such as online piracy and peer to peer file-sharing, and targeted or so-called 'behavioural' advertising." The view was again expressed in the Digital Report that the UK government's preference remains for an effective self-regulatory approach in relation to online content safeguards. The report also acknowledged that the UK industry "has taken some important steps forward and that a number of self-regulatory initiatives are taking place".[91]

To date, there are two main approaches in eliminating online child sexual abuse content in the context of self-regulation: internet blocking & notice and take down.

3.3.2 Internet Blocking

3.3.2.1 Internet Blocking in the Context of Child Sexual Abuse Content

Internet blocking has different approaches. Personal filtering and network blocking are the most commonly used applications whereas hybrids of these two styles are also in use, e.g. route filter.

Internet blocking (sometimes called filtering) refers to technical measures applied across all or some of an ISP's services and technology platforms in order to prevent inadvertent access to potentially criminal child sexual abuse content and to disrupt both casual consumers of child sexual abuse content and determined paedophiles. Although exchange of child sexual abuse content also takes place via other means, such as peer-to-peer applications and emails, the blocking measures adopted by ISPs so far focuses more on websites that are suspected of containing potentially criminal content of child sexual abuse. Therefore, such blocking does not deal with exchange of child sexual abuse content through peer-to-peer file-sharing platforms.

ISPs use internet blocking to disrupt viewing of child sexual abuse content through their servers and to make it difficult for users to view blocked sites containing child abuse materials, whichever country the sites are hosted in. Where blocking is undertaken by ISPs, it is mainly via voluntary agreements between ISPs and authorities. For example, in the UK, about 98.6% of the UK ISPs have adopted the IWF blacklist to block access to potentially criminal content hosted abroad.[92] UK

[91] See Department for Culture, Media and Sport And Department for Business, Innovation and Skills, June 2009, "Digital Britain Final Report", Chapter 7, para 60.
[92] See, A Campbell, Hansard HC vol 497 col 1546W (21 October 2009), available at

Government officials have also spoken widely on the Government's positions and expectations regarding the blocking of online child sexual abuse content since 2006 and have reiterated the government's intention to ensure that the remaining UK ISPs take steps to block with legislation being an option if blocking is unachievable through self-regulation.[93] In addition, the IWF blacklist has been deployed by companies in many countries around the world including internet service providers, mobile operators, search providers and filtering companies, such as, Google, Bing and Yahoo – three of the largest U.S. - based search engines.[94] In France, an agreement was reached between the French government and French ISPs for blocking sites carrying certain content including child sexual abuse content in June 2008. Whereas, CIRCAMP (COSPOL Internet Related Child Abusive Material Project), a system developed for blocking entry to known child sexual abuse content sites by a red stop sign graphic and a message – has now been used in several European countries including Denmark, Finland, Italy, Malta, Norway and Sweden.[95]

Apart from internet blocking on a voluntary basis, governments of many countries have also been considering whether to regulate their internet blocking activity on child sexual abuse content; however, only a handful of countries have a legal requirement for ISPs to block child sexual abuse sites. For instance, in Italy it is now compulsory under law to block child abuse websites. The Centre against Child Pornography on the Internet in Italy maintains a list of sites to be blocked and shares the list with ISPs that have 6 hours to block a site newly added to the list.[96] Pornographic sites are also blocked in South Africa[97] where ISPs are required by law to block the dissemination of child sexual abuse images. In Japan, the Japanese Government has recently announced measures to help stop child sexual abuse, including requiring ISPs to block access to indecent images of children on the internet and setting up a new body responsible for compiling a list of websites containing contents that violate Japanese laws banning child prostitution and child sexual

http://www.publications.parliament.uk/pa/cm200809/cmhansrd/cm091021/text/91021w0024.htm (last visited on 22 September 2010)

[93] See UK House of Commons Debates, "Offences Against Children: Internet", available at http://www.publications.parliament.uk/pa/cm200809/cmhansrd/cm091102/text/91102w0017.htm#09110238000131 (last visited on 20 September 2010)

[94] See IWF, "Combating Online Child Sexual Abuse Content at National and International Levels: IWF Experience, Tactical Suggestions and Wider Considerations", 26 July 2010, available at http://www.iwf.org.uk/media/page.70.636.htm (last visited on 20 September 2010)

[95] See CIRCAMP, "How Many Countries are Blocking Child Pornography on the Internet?", http://circamp.eu/index.php?view=items&cid=1%3Ageneral&id=17%3Ahow-many-countries-are-blocking-child-pornography-on-the-internet&option=com_quickfaq&Itemid=9

[96] See European NGO Alliance for Child Safety Online, (April 2009), "Using Blocking to Combat Online Child Abuse Images: Questions & Answers", p.2.

[97] See *supra* note 4, p.14.

abuse.[98] In Singapore, the Media Development Authority of Singapore also maintains a confidential list of blocked websites containing pornographic contents.[99]

In Europe, the European Commission has submitted a proposal to introduce blocking measures for stopping access to child sexual abuse content internet websites at the European level. According to Article 21 (1) of the draft Directive on Combating Sexual Abuse, Sexual Exploitation of Children and Child Pornography, Repealing Framework Decision 2004/68/JHA,[100] [M]ember States shall take the necessary measures to obtain the blocking of access by internet users in their territory to internet pages containing or disseminating child sexual abuse content while providing adequate safeguards to relevant parties such as internet users and content providers. The origin text of Article 21 (1) has caused much controversy as it appeared to require Member States to block access to web pages containing or disseminating child sexual abuse content. Despite this Article having been modified in the latest version of the draft Directive, it leaves Member States to decide exactly how the blocking should be implemented, whether through legislation or non-legislative measures, it remains to be seen whether or not the Article will finally be adopted.

3.3.2.2 The Advantages of Blocking and Incentives behind Blocking

Internet blocking, if technically effective, has the potential to limit accidental access to sites containing child sexual abuse content and therefore prevent users accidentally stumble across child sexual abuse content. More specifically, internet blocking has a number of advantages:

Firstly, internet blocking can create obstacles for innocent users to stumble across child sexual abuse content and therefore prevent accidental access to such content.

Secondly, blocking access to child sexual abuse content websites can make it harder for those who do not have much knowledge about accessing child sexual abuse material but who are curious, or are intended to develop their sexual interest in children and may turn to be potential child sexual abuse offenders.

[98] See Japan Today, "Gov't to Have Internet Providers Block Access to Child Porn Images", 27 July 2010, available at: http://www.japantoday.com/category/national/view/govt-team-oks-plan-to-get-isps-to-block-access-to-child-porn-images (last visited on 29 September 2010)
[99] See Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, editors, Access Denied: The Practice and Policy of Global Internet Filtering, London, England: The MIT Press, 2008, p. 3.
[100] See Proposal for a Directive on Combating Sexual Abuse, Sexual Exploitation of Children and Child Pornography adopted by the European Commission on 29 March 2010, available at http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/107 (last visited on 20 September 2010)

Thirdly, when blocking is in place, attempts to access blocked sites containing child sexual abuse content can generate data and can be recorded by ISPs. Such data may be used by law enforcement for possible criminal investigation. The statistics [101] released by the UK's largest broadband supplier BT in April 2009 suggested that there were between 35,000-40,000 attempts to access sites on the IWF blacklists each day via BT Retail's broadband network though it is hard to judge the percentage of deliberate attempts or attempts by accident or those by automated computer programs.

Because internet blocking has certain advantages in disrupting the availability of online child sexual abuse content, internet blocking remains as an option. It is particularly attractive to those, either domestic governments or individual ISPs, that look for a simple and effective means to protect their users from accidental access to potentially criminal child sexual abuse contents, in particular, content is often located beyond the jurisdiction of one country or where the ISPs base their operations. The incentives behind internet blocking can be identified as follows:

First, for countries that have poorly functioning law or have no laws on child sexual abuse related offences, when their social responsibility and moral responsibility require them to take action against proliferation of child sexual abuse content; blocking access to such content could be an easier way to tackle the problem.

Second, for countries that already have legislation and regulatory regimes for child sexual abuse related crimes but have no jurisdiction over such content hosted by countries that have no hotline and international co-operation on cybercrime with whom is not effective, internet blocking is the means to protect their internet users from exposure to child sexual abuse content. The deployment of the IWF blacklist in the UK is an example.

Third, differences between the laws regarding child sexual abuse related offences could make one country or ISPs in the country adopt blocking mechanisms to block child sexual abuse content that may not be criminalised in another country but is illegal in their country.

Internet blocking does have certain advantages and it has a crucial role to play both in disrupting the domestic users' exposure to child sexual abuse materials and in preventing child sexual abuse related crimes. However, internet blocking also has its

[101] See Chris Williams, 7 April 2009, "BT Blocks up to 40,000 Child Porn Pages Per Day: Cleanfeed Busy", available at http://www.theregister.co.uk/2009/04/07/bt_cp_figures/ (last visited on 21 September 2010)

weakness and this is the reason why internet blocking has attracted so much controversy.

3.3.2.3 Problems with Internet Blocking

Despite its benefits, there are controversies surrounding internet blocking not only generally, but also in regard to child sexual abuse content. The controversy concerns particularly internet users' privacy, freedom of expression, and other technical issues affecting the effectiveness of blocking. In addition, the cost for ISPs by the adoption of internet blocking services is also a factor that should be taken into consideration.

First, there are two issues reflected in the heated debate[102] concerning internet blocking introduced by Article 21 (1) of the draft Directive on Combating Sexual Abuse, Sexual Exploitation of Children and Child Pornography, Repealing Framework Decision 2004/68/JHA.

The first issue is the conflict between internet blocking and the right of respect for private and family life. Right to respect for private and family life is considered as a fundamental freedom. According to Article 8 of the European Convention on Human Rights (the ECHR), "everyone has a right to respect for his private and family life, his home and his correspondence", with exception to certain restrictions that are "in accordance with law" and "necessary in a democratic society". However, the adaptation of internet blocking/filtering measures for preventing access to child sexual abuse content means that users' communication and behaviours over the internet may be monitored, the retention of internet data without permission may be required, and the users may not be able to make their own connection choice to other users or to create certain connections.

Freedom of expression is another concern for those who oppose internet blocking because internet blocking may result in some users being deprived of a right of accessing content or the right to make certain content available online. As a fundamental right provided by the Universal Declaration of Human Rights (the UDHR), the International Covenant on Civil and Political Rights (the ICCPR) and the European Convention on Human Rights (the ECHR), the right to freedom of expression entitles people to receive information by any means including internet. While some may argue that internet blocking may limit the accessibility of certain content and may

[102] See Peter Hustinx, "Opinion of European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on Combating Sexual Abuse, Sexual Exploitation of Children and Child Pornography, Repealing Framework Decision 2004/68/JHA, 10 May 2010. Also see, European Digital Rights, "ENDitorial: Internet blocking in ten weeks and counting", EDRi-gram - Number 8.18, 22 September 2010.

therefore limit users' rights to freedom of expression, it shall be noted here that the above mentioned international legal instruments do not give preference to freedom of expression over other rights including the rights of children though a balance must be achieved.

Secondly, internet blocking does not facilitate police investigation and prosecution of child sexual abuse content and the offenders behind such content. Also, internet blocking does nothing to help identify and protect children appearing in child sexual abuse images. Therefore, blocking cannot put an end to offenders abusing children.

In addition, internet blocking can be ineffective due to over-blocking and/or under-blocking. Although it is said that internet blocking began over twenty years ago with the blocking of unsolicited emails (spam), [103] over-blocking and under-blocking remain as problems that affect its accountability and transparency. Over-blocking occurs when a filter incorrectly prevents users' access to legitimate contents, or, when a site that should not be blocked is added to the list. The IWF Wikipedia incident[104] is an example of over-blocking. In the IWF Wikipedia incident, the IWF were accused of blacklisting pages on Wikipedia, which led to over-blocking and causing difficulty for internet users to edit information on Wikipedia. Although the IWF claimed that they were very careful about compiling and handling their blacklist and the incident happened because of an unforeseen technical side effect of blocking, the IWF board finally decided to remove the specific URL from their blacklist to avoid over-blocking. [105] Over-blocking can result in the difficulty of users to access information they need and make their own connection choice but over-blocking cannot be completely prevented based on a recent internet blocking study [106]. Sometimes, criticism on over-blocking may turn ISPs' over-blocking to under-blocking due to ISPs' legal entanglement concerns. When a filter works without human judgement and incorrectly allows access to the content that should be blocked, it can result in under-blocking. Under-blocking can increase the opportunity of allowing the users to access unlawful online content including child sexual abuse materials. As is in the case of the IWF, after the Wikipedia incident, the IWF has now

[103] See Cormac Callanan, Marco Gercke, Estelle De Marco, and Hein Dries-Ziekenheiner, "Internet Blocking - Balancing Cybercrime Responses in Democratic Societies", October 2009, available at http://www.aconite.com/sites/default/files/Internet_Blocking_and_Democracy_Exec_Summary.pdf (last visited 24 September 2010), p. 10.
[104] See IWF, "2008 Annual and Charity Report", available at http://www.iwf.org.uk/documents/20091214_iwf_annual_report_2008_pdf_version.pdf, p.9
[105] ibid.
[106] See *supra* note 103, p.12.

changed their tactics when implementing blocking,[107] which could possibly lead to some under-blocking.

Internet blocking not only has the potential for over-blocking and under-blocking, it can also be circumvented, in particular, by those determined to access child sexual abuse content. As Dr Richard Clayton pointed out[108], all network-level blocking could be overcome, either by encrypting content or by using proxy services hosted outside of one jurisdiction. Further research[109] concerning internet blocking also indicated that, the potential of internet blocking to be circumvented is very likely although how easy the circumvention is may depend on the medium adopted. In addition, internet blocking is inefficient against exchange of child sexual abuse content via closed networks, such as emails and peer-to-peer file sharing.

The ineffectiveness of internet blocking is not only because of the above issues, but because internet blocking does nothing to take down child sexual abuse content at the source. Internet blocking makes access to child sexual abuse content difficult, it still leaves child sexual abuse content online and the sites accessible for anyone who is determined to see it.

Besides, the implementation of internet blocking technologies would imply additional costs for ISPs. ISPs therefore may determine whether to perform blocking measures based on their calculation of the costs.

3.3.2.4 Summary

It is suggested in the above discussion and other studies[110] that internet blocking is considered as one of the means to prevent access to child sexual abuse content. However, internet blocking by self-regulation has received as much criticisms as internet blocking under state regulation has. While some strongly doubted the accountability and transparency of internet blocking operated by private parties, others argued that internet blocking underpinned by law may also interfere with users' privacy and freedom of expression.

---

[107] See *supra* note 94, p.6, 10.3
[108] See Richard Clayton, "Failures in a Hybrid Content Blocking System", presented at the Workshop on Privacy Enhancing Technologies, Dubrovnik, Croatia, 30 May 2005 -- 1 June 2005, available at http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf.
[109] See *supra* note 103, p.118.
[110] For example, see Cormac Callanan, Marco Gercke, Estelle De Marco, and Hein Dries-Ziekenheiner, "Internet Blocking - Balancing Cybercrime Responses in Democratic Societies", October 2009, available at http://www.aconite.com/sites/default/files/Internet_Blocking_and_Democracy_Exec_Summary.pdf (last visited 24 September 2010)

Internet blocking can be very useful in preventing users from accessing the sites containing child sexual abuse content and undermining viewing, distribution and commercial trade of child sexual abuse content over the internet if we put the concerns aside. However, the controversy surrounding internet blocking makes it simply a disruption tactic to the availability of child sexual abuse content, rather than a preferred option for removing child sexual abuse content at source. To definitively remove online child sexual abuse content, a more effective solution needs to be implemented and a notice and take down system could be the answer to the problem.

3.3.3 The Notice and Takedown System

3.3.3.1 The Notice and Takedown System in the Context of Child Sexual Abuse Content

The notice and takedown system is another self-regulatory model [111] developed through the work of hotlines that allow members of the public to report potentially unlawful child sexual abuse content so that such content can be quickly removed. Receiving reports, assessing content in the reports, tracing content concerned and issuing notices to relevant parties or informing law enforcement body for taking down content are all involved in the operation of a notice and takedown system.

As discussed in Part 2 of the report, hotlines are operated by different organisations in different countries. Industry-run and child welfare-run and public body-run hotlines are typical models among them. Although the functions and procedures of each hotline differ depending on national law and social circumstances, child sexual abuse content is one of the major concerns of all hotlines and notice and takedown is the main procedure adopted in the operation of the hotlines.

While the hotlines are gradually established in a number of countries, international co-operation between these countries' hotlines is also growing, especially within the network of INHOPE. Member hotlines of INHOPE are sharing information and experience, supporting an international development of new hotline initiatives, improving the ways of exchanging intelligence regarding illegal content, and working together to promote awareness of the challenges posed by the internet and developing technology. In the context of eradicating child sexual abuse content on the internet, member hotlines exchange their intelligence by passing details to their INHOPE hotline partner in the hosting country so they can work with local police to investigate the content and take the content down within their national legislation.

[111] This does not necessarily mean that notice and takedown procedure is simply a self-regulatory model as such a procedure is also mandated by the law in Australia for combating child sexual abuse content.

At the European level, the notice and takedown approach is well in line with the spirit of EU law as, for example, illustrated by the 2000 Directive on Electronic Commerce, which encourages industry self-regulation to implement a notice and takedown system. The Council Decision 2000/375/JHA of 29 May 2000 to Combat Child Pornography on the Internet also requires Member States to take measures to encourage the reporting of child sexual abuse content and ensure law enforcement authorities react rapidly after receiving information on alleged cases of the production, processing, distribution and possession of child sexual abuse content. The Council Decision encourages the sharing of a list of 24-hour national contact points and specialised units between Member States in order to facilitate cooperation, which implies the involvement of a notice and takedown procedure. In addition, the EU Safer Internet Programme has also provided funds for INHOPE and some of their member hotlines.

There are still countries where hotlines do not exist, and this becomes a worrying concern that the dissemination of child sexual abuse content in these countries might be difficult to prevent while a notice and takedown system is not in place.

3.3.3.2 The Strengths of the Notice and Takedown System

There are several reasons that the notice and takedown procedure is now a widely endorsed regulatory system for child sexual abuse content. The most important is because the procedure enables the swift removal of child sexual abuse content at the source. Many countries' hotlines not only identify, assess and trace potentially criminal child sexual abuse content, they issue takedown notices to relevant ISPs. They also have a monitoring process to check if the reported content has been taken down to make sure that the notice and takedown procedure can really put an end to the circulation of online child sexual abuse content. The notice and takedown procedure has now proved extremely successful, particularly in removing child sexual abuse content domestically. According to the IWF, websites hosted in the UK are removed within an hour following a notice from IWF to the hosting provider[112] and child sexual abuse content hosted in the UK has reduced from 18% in 1997 to less than 1% since 2003[113]. Despite 40 instances of child sexual abuse content hosted in the UK being reported in 2009, all of the content was promptly removed within a day

[112] See *supra* note 94, p.3, 5.2.
[113] See IWF, "2009 Annual and Charity Report", available at: http://www.iwf.org.uk/documents/20100511_iwf_2009_annual_and_charity_report.pdf, p.10.

by the ISPs concerned upon noticed by the IWF and evidence was preserved for police investigation.[114]

In Australia, statistics[115] from ACMA also shows that the proportion of Australian hosted child sexual abuse content has diminished significantly over the past ten years. In the period 1 January 2000 to 31 December 2002, the Australian Broadcasting Authority (one of ACMA's predecessors) had issued 95 takedown notices to Australian ISPs regarding complaints about child sexual abuse content. Only a total of 68 takedown notices were issued for child sexual abuse content hosted in Australia in four years, during the period 2003 to 2007. Takedown notices issued counted only 21 in the period 2008 to 2009; whereas no takedown notice has been issued in 2010.

In the U.S., the development and implementation of a Notice Tracking System has also ensured that the length of time that an electronic service provider continues to host apparent child sexual abuse content after notification is monitored and the length of time that the apparent child sexual abuse content remains available on the URL after notification is reduced.[116]

The feedback from countries participated to our survey also suggests that the notice and takedown procedure run by the hotlines has greatly diminished the dissemination of online child sexual abuse content. As a German hotline observed, online child sexual abuse content has decreased significantly due to the work of the hotline and child sexual abuse content hosted in Germany has been taken down within hours.[117] Spanish hotline – Protegeles also noticed tremendous decrease of child sexual abuse content over the Spanish internet territory in the past ten years.

Additionally, part of the notice and takedown procedure such as tracing content supports police investigation and helps the identification of new child sexual abuse sites. Once potentially criminal child sexual abuse content is identified, the hotlines will alert law enforcement bodies of the content. Then the police can identify criminal child sexual abuse content, hosting websites and child victims as well as gather evidence and prepare for criminal investigation. According to a survey conducted by INHOPE, 14 out of 21 members' hotlines that responded to the online survey have a "Memorandum of Understanding" (MOU or equivalent) with their police relating to

[114] *Ibid*, p.15.
[115] See ACMA, Online Content Complaint Statistic from 2001 – 2010, available at: http://www.acma.gov.au/WEB/STANDARD/pc=PC_90105 (last visited on 27 September 2010)
[116] See INHOPE, "2010 INHOPE Autumn Newsletter", pp.5-6.
[117] See eco, "The eco Internet Complaint Hotline Results 2009-2010", August 2010.

procedures in communication of notice & takedown to ISPs.[118] The 2009 report[119] submitted by the Special Rapporteur (Ms. Najat M'jid Maalla) suggested that the work of the hotlines "have frequently led to the identification and blocking of new child sexual abuse content sites (2,500 in Switzerland; 164 in Italy; 532 in the Netherlands; 1,864 in Japan, etc.)." Over the years, intelligence gathered by the hotlines enabled many successful national and cross-border police investigations and operations. For example, in the UK, the IWF works in close liaison with different police forces and national UK police agencies and has provided statements and intelligence to support investigation and prosecution to the police. In 2009, the IWF provided 11 evidential statements and specific intelligence to the police for investigation on 80 occasions. In addition, in 2009 the IWF assisted with ongoing investigations in many countries including the US, Egypt, and France.[120] In Spain the Protegeles hotline referred intelligence in relation to child sexual abuse content to the police and enabled many national and international police operations, including Operation Marcy (involving Spanish and German hotlines and law enforcement agencies), Operation Tarragona, Operation Comunidades, and Operation Anamtomía.[121]

Intelligence analysis as part of the notice and takedown procedure also helps identify and rescue of abused child victims to prevent re-victimisation of the children who are or have been the victim of abuse. In the UK, the IWF has been referring images and videos to CEOP so that the CEOP experts can identify child victims in the UK or abroad, 80 police investigations were initiated as the result of specific intelligence analysis provided by the IWF to CEOP.[122] There are also many success stories in other countries, such as in the U.S.[123], regarding children being removed from abusive situations as the result of the intelligence analysis provided by the hotlines.

3.3.3.3 The Drawbacks and Limitations of the Notice and Takedown System

While the notice and takedown approach has significant benefits, it also has its drawbacks. Particularly if the implementation of such a model does not comply with the law or the implementing body bypasses the official law enforcement route while issuing takedown notices. The major concern in this regard is the impact of the notice

[118] See INHOPE, "Notice & Takedown Survey 2010 - Results", Question 11.
[119] See *supra* note 4, p.18, para 91.
[120] See *supra* note 113, p.20
[121] See Protegeles, "Helpline", available at: http://www.protegeles.com/eng_que_hacemos1.asp (last visited on 12 October 2011)
[122] See IWF, "IWF Operational Trends 2009", available at: http://www.iwf.org.uk/resources/trends (last visited on 2 January 2011)
[123] See the National Centre for Missing & Exploited Children, "CyberTipline® Success Stories", available at: https://secure.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=376 (last visited o 29 September 2010)

and takedown procedure on police investigation, in particular, if a hotline issues a notice directly to ISPs without informing or consulting law enforcement agencies. The issuing of a takedown notice to the ISPs can lead to the effective and efficient removal of child sexual abuse content but it may undermine an ongoing or a potential police investigation. It may also result in the loss of forensic data as valuable evidence if adequate records regarding the potentially criminal child sexual abuse content are not maintained by ISPs. Nevertheless, in a number of hotlines' agreements with their law enforcement partners, such a concern has been addressed and the hotlines are required to keep the police informed prior to issuing notice to the ISPs. In Australia, the notice and takedown procedure has been made mandatory so the ACMA will only issue a takedown notice after confirmation from the police that doing so will not impact on a criminal investigation. However, such a concern may still be valid for countries that are at the early stage of implementing a notice and takedown system. For the hotlines that are intending to issue takedown notices directly to overseas ISPs without following the official law enforcement route, the possible negative impact of their notice and takedown procedures on police investigation should be minimised to avoid compromise of any judicial or law enforcement arrangements in place.

Another limitation of the notice and takedown system is that such a system is currently ineffective against distribution of child sexual abuse content through peer-to-peer file-sharing networks. Despite peer-to-peer file-sharing declining globally,[124] distribution of child sexual abuse content by the use of peer-to-peer file-sharing software makes it difficult to detect and intercept[125] and therefore the notice and takedown system becomes ineffective.

The emergence of alternative ways to distribute child sexual abuse content is also challenging the effectiveness of the notice and takedown system. For example, according to the IWF[126], the use of free hosting sites such as Megaupload and Rapidshare is now increasing. These sites have the advantage of offering free website hosting or free image sharing services and keeping content providers anonymous.

[124] See Ryan Singel, "Peer-to-Peer Passé, Report Finds Global Decline of P2P", 13 October 2009, available at: http://www.wired.com/epicenter/2009/10/p2p-dying/ (last visited on 2 January 2011)
[125] See P25, para 2, of the CEOP Strategic Overview 2009-2010, available at: http://www.ceop.police.uk/Documents/Strategic_Overview_2009-10_%28Unclassified%29.pdf (last visited on 13th February 2011) (It is said in the Strategic Overview that CEOP has set up a strategy group in an effort to understand the threat made by peer-to-peer file sharing which is recognised as the most frequently used environment for distributing indecent images while "[L]ittle is known about the nature and extent to which child sexual offenders use P2P and it continues to be an intelligence gap.")
[126] See *supra* note 122.

However, it is difficult to trace and identify those who produced and distributed child sexual abuse content through these new platforms.

3.3.4 Internet Blocking vs. Notice and Takedown

Having discussed the strengths and weaknesses of internet blocking and the notice and takedown procedure, it might be of concern whether internet blocking should be promoted or a standardised notice and takedown procedure should be encouraged and further developed in order to effectively reduce the dissemination of child sexual abuse content.

While internet blocking has the advantage of disrupting access to child sexual abuse content, the problem is that the adoption of internet blocking mechanisms may be in conflict with the right to respect for private and family life and the right of freedom of expression. In addition, when comparing internet blocking to the notice and takedown approach, internet blocking has no ability to facilitate police investigation and prosecution of the offenders behind the illegal content, nor can it identify and protect child victims appearing in child sexual abuse content. Those who are determined to access child sexual abuse content can always circumvent internet blocking. More crucially, internet blocking does nothing to remove the content at source and therefore it cannot put an end to child sexual abuse content. Hence, even though internet blocking can be taken as a means of disrupting access to child sexual abuse content, it cannot be a long-term solution for the eradication of child sexual abuse content in a rapidly advancing technology environment.

With the ultimate benefit of removing child sexual abuse content at source, the notice and takedown procedure also has drawbacks and limitations. However, while there is a wide international consensus that child sexual abuse content is illegal, the exercise of the right of privacy and freedom of expression would not be adversely affected to any great extent if the notice and takedown procedure is implemented proportionately and appropriately. The drawback of undermining ongoing or potential police investigation can also be overcome, for example, by facilitating an international agreement on establishing a standardised notice and takedown system for the swift and effective removal of child sexual abuse content, or through international organisations such as INHOPE, to provide a guideline for implementation of the notice and takedown procedure. As for dissemination of child sexual abuse content via peer-to-peer file-sharing and other emerging technologies, more advanced technologies may be developed to solve the problem in the near future.

Even when we encourage the development of a comprehensive international notice and takedown system, it does not mean that internet blocking should be abandoned. Whilst a wholly effective international notice and takedown system is not yet established, internet blocking can still be a short-term solution and can play a continuing role in disrupting access to child sexual abuse content.

Indeed, whilst there has been heated debate over the choice of internet blocking or the notice and takedown procedure, there is a consensus[127] that, the approach of removing child sexual abuse content from the internet at source takes precedence over the approach that prevents users from accessing such content, because deleting child sexual abuse content sites is more efficient than blocking them. The notice and takedown procedure is the way to achieve this result while internet blocking cannot do the same. In fact, the notice and takedown procedure is widely regarded internationally as the preferred model. It has proved effective in some places, and has proved workable across the EU where INHOPE members' hotlines exist in most European countries. However, the circulation of child sexual abuse content has a considerable cross-border dimension, therefore, effective international co-operation or an international standardised notice and takedown procedure is urgently needed to ensure that child sexual abuse content is taken down completely and effectively across the globe.

Nevertheless, the likelihood of developing an international notice and takedown system does not mean there are no barriers to developing high-level international agreement. Several factors need to be taken into consideration, among them, the differences between national standards relating to child sexual abuse content, differing legal procedures relating to takedown of child sexual abuse content, impact of the notice and takedown procedure on police enforcement activities related to child sexual abuse offences and safeguards for the "notice and takedown" body, ISPs and internet users.

3.4 Conclusion

When child sexual abuse content is disseminated in an increasingly interactive online environment, statutory regulation is no longer the only mechanism to tackle child sexual abuse content. It is widely recognised that ISPs and other organisations can

[127] See for example, the Proposal for a Directive of the European Parliament and of the Council on Combating the Sexual Abuse, Sexual Exploitation of Children and Child Pornography, repealing Framework Decision 2004/68/JHA, (13). Also see, BBC News, "Delete Child Abuse Websites Says German Minister", 31 March 2010, available at: http://news.bbc.co.uk/1/hi/technology/8596650.stm (last visited on 29 September 2010); European Digital Rights, "Deleting Illegal Sites is More Efficient than Blocking them", EDRi-gram - Number 8.17, 8 September 2010.

play a role in preventing availability and circulation of child sexual abuse content on the internet, therefore self - and co-regulation is encouraged in order to remove such content effectively at source.

Internet blocking and the notice and takedown procedure as the two main features of self-regulation have been implemented in eradicating online child sexual abuse content. However, both mechanisms have advantages and disadvantages. The notice and takedown system may have a negative impact on law enforcement arrangements if the "notice and takedown" body only aims to remove the content promptly without considering that such activity could undermine police investigation. In addition, the notice and takedown procedure is inefficient in preventing the dissemination of child sexual abuse content through emails and peer-to-peer file-sharing exchanges. The disadvantages of internet blocking on the one hand may impede the exercise of the rights of users' privacy and freedom of expression; whereas on the other hand, the potential of blocking being circumvented and over-blocking as well as under-blocking can really weaken transparency and accountability of internet blocking.

Notwithstanding the weaknesses of these two self-regulatory mechanisms, their strengths are undeniable. Internet blocking has been successful in disrupting availability of child sexual abuse content, in particular, for content hosted outside of one particular jurisdiction. Whereas the notice and takedown system has the outstanding merit of effectively removing child sexual abuse content at source without compromising the simultaneous capture of evidence necessary to investigate and prosecute offenders.

Having said that, it is no surprise that the 'notice and take down' system on internet sites has been widely regarded as the preferred model, although such a system was never devised as a panacea and still needs to be improved and further developed. It is understood that the prompt removal of child sexual abuse content at source is one key element in a layered approach to combating child sexual abuse images online and nobody has challenged the need to develop a strong and effective framework to fight against child sexual abuse content on the internet. Therefore, it is appropriate to say that efforts should be made urgently to strengthen and develop an international notice and takedown system, rather than making internet blocking compulsory, so that a global problem can be solved by a global solution.

This report has no intention of overlooking the drawbacks of the notice and takedown procedure nor has it the intention to understate the obstacles pertaining to the further development of an international notice and takedown system. It is the

author's view that only if the obstacles can be eliminated and the existing notice and takedown system is improved, such a system will secure its benefits and will be deemed efficient. Therefore, if an international notice and takedown system were to be further developed and effectively implemented, there are a number of issues that need to be considered and addressed.

Part 4: The Development of an International Notice and Takedown System

4.1 Introduction

As discussed in Part 3, the notice and takedown procedure as a widely recognised model for effectively removing online child sexual abuse content has played a crucial role in a strategy designed to achieve the expeditious removal child sexual abuse content hosted, in particular, within the countries that are members of the INHOPE network. The success of the notice and takedown procedure also indicates the potential for developing a transferable model of international notice and takedown for the large scale distribution of online child sexual abuse content. While the means of distributing child sexual abuse content are diversifying with further advancement of the internet and digital technology, a global solution is therefore needed to tackle the proliferation of child sexual abuse content, which is a global problem.

Nevertheless, the success of the notice and takedown system in one particular country or within a particular region does not necessarily mean that such a model can be equally successful at an international level. It will be useful to consider elements that may impede further development and implementation of an international notice and takedown system, in particular, differences between countries' legislations and legal procedures, the extent of international cooperation, the impact of such a system on police enforcement activity as well as potential risks to an organisation that issues takedown notices.

This part begins by discussing the necessity and possibility of further developing an international notice and takedown system. It then analyzes several influential factors in developing such an international notice and takedown system. While the research is not intended to provide a complete answer on how to minimise the impact of the influential factors on the development of an international notice and takedown system, it is however the intention of the research that the issues discussed should be taken into consideration in the course of developing a comprehensive, transferable international notice and takedown system so that the effective removal of child sexual abuse content can be ultimately achieved at an international level.

4.2 The Necessity and Possibility of Developing an International Notice and Takedown System

An international notice and takedown system relating to online child sexual abuse content refers to a system that allows a hotline in one country to issue notices to other countries through the hotlines or other trusted organisations or to issue

advisory takedown notices directly to overseas ISPs under certain circumstances, e.g. after notifying hotlines or other trusted organisations for a certain period of time but receiving no response. Such an international notice and takedown system may also include a process that allows a hotline to issue advisory notices to international ISPs in a country that does not have a hotline capable of assessing illegal content in their country. However, such an attempt should only be made after the hotline notifies a foreign law enforcement agency of potentially illegal child sexual abuse content via their national police and/or other international law enforcement bodies such as Interpol. Such takedowns should only be performed after international ISPs have consulted with their domestic law enforcement bodies and on the basis of their domestic legislation. The implementation of such an international notice and takedown system shall not compromise any protocols between hotlines and statutory authorities in other countries and the law enforcement activities in the case that the notice has been sent directly to ISPs in a country that a hotline does not exist. The aim of an international notice and takedown system is to reduce the availability of child sexual abuse content on the internet and reduce the number of children who are sexually abused or re-victimised by facilitating expeditious removal of child sexual abuse content from the internet at its source, wherever that content is hosted.

The necessity of an international notice and takedown system relating to online child sexual abuse content is based on the following reasons.

Firstly, while the internet has offered many opportunities for international communication, it has also created a platform for those who produce and distribute child sexual abuse material across borders. The distribution of online child sexual abuse content is considered a serious crime because it has a significant impact on the physical and mental health, re-victimisation, safety and well-being of children. Every time the image is viewed online or it is downloaded, the child victim in it is being re-abused. In addition, there is a risk that people who have not previously engaged with child sexual abuse content might find the content and develop an interest in it. Therefore, to remove child sexual abuse content at its source is vital, particularly in terms of online child protection and eradication of child sexual abuse related crimes.

The amount of child sexual abuse content hosted domestically has been greatly minimised in some countries and a notice and takedown procedure is proven to have contributed to that. It is striking that there is still a great deal of child sexual abuse content available over the internet worldwide and the scale of all child sexual abuse content online is difficult to measure because the methods of distribution are

changing with the emergence of new technologies.[128] According to the IWF 2009 report, during 2009 the IWF dealt with 8,844 child sexual abuse content instances hosted around the globe, with identified URLs on 1,316 different domains. Almost half the sexual abuse content URLs identified were located on 14 hosting providers with two providers each hosting 7% of the total 8,844.

Although the overall number of domains on which this content is found has decreased by 57% since 2006, the number of URLs with child sexual abuse content known to the IWF remained fairly stable in the period of 2006 -2009.[129] Among the 8,844 confirmed instances of child sexual abuse content, there were 4,199 child sexual abuse URLs being hosted in the countries of North America, whereas Europe (including Russia) hosted 3,932 child sexual abuse URLs. The rest were hosted respectively in Asia (644), South America (65), and Australia (4).[130] Due to the fact that such content reported to the IWF was not generally hosted in the UK, the IWF has no competence to assess the illegality of the content against the laws in the hosting country and issue takedown notices. While the IWF can block the access to the content to prevent the exposure of UK internet users, the content is very likely to be circulated all over the internet if the country hosting such content does not take them down.

According to ACMA, the proportion of child sexual abuse content hosted beyond the Australian internet territory know to ACMA has also increased from 845 referrals between 2005 and 2006 to 1,189 referrals during 2007-2008. In the period 2009-2010, 1,924 referrals have been made to the makers of filters for blocking access.[131] This indicates there has still been an increase of child sexual abuse content hosted abroad known to ACMA but beyond of the jurisdiction of the ACMA. This may be due to two reasons: (a) internet blocking/filtering mechanism adopted by the Australian accredited filter software providers has not been that effective; and (b) in the absence of a well-developed international notice and takedown system, child sexual abuse content hosted overseas cannot be removed at the source so that the content could be distributed again over the internet.

It was also discovered in a study conducted by the Canadian Centre for Child Protection in November 2009 that 49.2% of the 12,696 websites hosting child sexual

[128] See *supra* note 113, p.8 (According to the report, "the distributers are increasingly using legitimate internet services to make the images available: from free hosting platforms and image sharing websites to social networking areas and hacked websites.")
[129] *Ibid*, p.15.
[130] *Ibid*, p.16.
[131] See ACMA, Online Content Complaint Statistic from 2001 – 2010, available at: http://www.acma.gov.au/WEB/STANDARD/pc=PC_90105 (last visited on 27 September 2010)

abuse content processed by Cybertip.ca were traced to the U.S., while 20.4% of the sites were traced to Russia. Canada remains the third country that hosted such content, with Japan and South Korea are the fourth and fifth respectively. [132]

It is evident that there is still a lot of child sexual abuse content available online, not only in the countries that do not have an established system for the swift removal of child sexual abuse content, but also in the countries that already have a notice and takedown system in place. According to CyberTipline's Annual Report Totals by Incident Type[133], reports concerning possession, manufacture, and distribution of child sexual abuse content steadily mounted during the period of 2006-2008, with 62,480 instances reported in 2006, 83,959 instances reported in 2007, and 85,301 instances reported in 2008. Apart from the steady increase of child sexual abuse content, the length of time some websites distributing child sexual abuse content remain available around the world is another particular concern for countries that have an established notice and takedown system but are unable to alert illegal content known to them where a partnership has not been established.

In December 2010, the U.S. CyberTipline claimed that they sent 1,042 notices pertaining to 759 URLs to Electronic Service Providers after content concerned were reported to them. On average, the URLs were removed in 2.36 days by Electronic Service Providers after receiving the NCMEC notification.[134] Nevertheless, efficient takedown may not be guaranteed for content hosted overseas because there is a process to be followed if the reports need to be sent via other routes such as INHOPE network or Interpol.

Secondly, whilst national governments have the primary responsibility to act to protect all children and tackle child sexual abuse related crimes within their jurisdiction, it is unrealistic to rely on one country's power to deal with child sexual abuse content being circulated across borders on the internet. There is therefore a need to have international institutions leading and encouraging action at an international level, or to have a standardised international system for the effective removal of child sexual abuse content at source.

Thirdly, statutory regulation at the international level has proven to have played a significant role in combating child sexual abuse content related crimes. However,

[132] See *supra* note 29, p.44.
[133] See CyberTipline, "Annual Report Totals by Incident Type", available at http://www.missingkids.com/en_US/documents/CyberTiplineReportTotals.pdf (last visited on 27 September 2010
[134] See CyberTipline: Monthly Notice and Take Down Update (December)

given the extent of online child sexual abuse content, relying on statutory regulation alone to address and tackle the problem is impossible. Because the law enforcement authorities have specific local and regional priorities, the focus is very often on prosecuting child sexual abuse related offenders rather than getting the content expeditiously removed.

The operation of hotlines in various countries, in particular, the work of the INHOPE hotlines has proven that the notice and takedown procedure has played a significant role in minimising the availability of child sexual abuse content and have been a critical first line of defence against child sexual abuse content online. With the support of the INHOPE network, national hotlines have been working together by sharing and managing intelligence and reports so that appropriate action can be taken against child sexual abuse content reported in one country but hosted in another. With 39 member hotlines in 34 countries from Europe, Asia, North America, Africa, Russia and Australia, INHOPE has also helped to develop and support national protocols for notice and takedown process, which take reports of illegal content, identify, confirm the existence and trace such content in order to have it eventually removed if they are deemed as potentially criminal. By now, the notice and takedown procedure has become a common practice in most of the INHOPE member countries, whilst it is also considered by countries that do not have such facility but in the meantime face the challenges posed by the proliferation of online child sexual abuse content.

In fact, the development of a notice and takedown system has also been encouraged at an international level. In the 2005 [135] and 2009 [136] reports, the UN Special Rapporteur commended the work of the INHOPE network in disrupting the circulation of online child sexual abuse content through a notice and takedown procedure and stressed the importance of international collaboration in fighting against online child sexual abuse content. Recently, the European Commission is also in consultation with INHOPE member's hotlines regarding Guidelines for Co-Funded Hotlines on Notice and Takedown, which would provide an example for developing guidelines for hotlines on notice and takedown at an international level.

While the availability of child sexual abuse content on the internet is still increasing, there is yet a need of an effective way to detect and remove such content in a timely manner across borders so as to prevent further circulation of the content and re-victimisation of child victims. The experience of several individual countries and the

[135] See *supra* note 3, p.21.
[136] See *supra* note 4, pp. 17-18.

work of INHOPE suggest that it is possible to transfer the existing notice and takedown procedure operated domestically and at regional level into a consistent and coordinated international notice and takedown system in order to effectively tackle this cross-border problem. Nevertheless, it is important to recognize that the advancement of a comprehensive, transferable international notice and takedown system is not an easy task to achieve and several factors may have an impact on the development of such a system. To help develop a workable international notice and takedown system and to ensure such a system can be effectively implemented, five influential factors are examined in the following context.

4.3 Several Pertinent Issues in Relation to the Development of an International Notice and Takedown System

While there is a broad consensus that the removal of content at source is the most effective way of combating online child sexual abuse content, several issues in relation to the takedown of child sexual abuse content are identified in the discussion of further developing such a notice and takedown system, which may also suggest why the implementation of a notice and takedown system has been slow to be adopted at an international level. Variations in national law and legal procedures that give rise to difficulties in effectively taking down child sexual abuse content on a global scale are definitely the deciding factors. Nevertheless, there are other elements that may have impact on the further development and implementation of a notice and takedown system internationally, including, for example, the extent of international cooperation, the impact of such a system on law enforcement activity as well as potential risks faced by the organisations issuing takedown notices.

4.3.1 Different National Standards relating to Child Sexual Abuse Content

Despite the efforts made by individual countries and the INHOPE network in removing child sexual abuse content on the internet, takedown of child sexual abuse content is still slow. Differences in national standards relating to child sexual abuse content can be one of the obstacles that result in the inefficiency of international co-operation in taking down such content across the globe.

According to a study[137] conducted by ICMEC in 2010, only 45 of the 196 countries around the world have legislation sufficient to combat child sexual abuse related offences. There have been legislative changes and movement in a number of countries, but there are still nations that have no legislation at all that specifically address child sexual abuse content and related offences, according to the Special

[137] See *supra* note 31.

Rapporteur 2009 report. In their jurisdictions, pornography is considered to be "an offence against public morals and decency or a violation of public order" and therefore child sexual abuse related offences are penalised in that context.

In the countries that have legislation addressing child sexual abuse content related offences, definitions differ, in particular, with respect to age of a child, definition of child sexual abuse content, scope of activities considered criminal as well as legal responsibility of internet service providers. As a result, the images of children that are deemed illegal in one country may actually be legal in the country of origin and therefore the takedown of such content may be problematic and not possible.

Differences in age threshold are one of the difficulties facing international co-operation relating to child sexual abuse content. For instance, in the majority of the top 15 countries hosting child sexual abuse content[138], a child is defined as a person under 18 years of age. In Canada, age of a child is 18 or 19, depending on the law of the provinces.[139] In Germany, the age threshold of a child is even younger at 14, although a person between 15 to 18 years of age is considered as a juvenile and is also especially protected by law. In addition, some countries take into account the age of criminal responsibility or the age of consent to sexual activity, which may vary between 13 and 16. For example, in Spain, the age of consent is 13 years old; however, the age threshold of a child is 18 years of age. Arguably, a child under 18 may be able to freely consent to sexual relations, but at such a stage he/she cannot be considered to be able to consent to any form of sexual exploitation including child sexual abuse. Therefore, variations in definitions of the age of consent and the age of a child make it difficult to determine the illegality of child sexual abuse content and take further action against it, and it is very likely to compromise a consistent and harmonised protection of children from sexual exploitation on an international level.

Definitions of child sexual abuse content (child pornography) also differ in different countries. For example, in the countries that responded to our survey questionnaire, only the U.S., Brazil, and Australia have defined child sexual abuse content in a specific legislation. Among them, the U.S. is the only country that has clearly defined all forms of internet child sexual abuse content. Other countries, such as, the UK, Spain, Germany, Taiwan, and Thailand do not provide a specific definition of child sexual abuse content in their legislation, although general provisions regarding

[138] See *supra* note 29, p.44. (This report identified the U.S., Russia, Spain, the Netherlands, the UK, Portugal, Czech Republic, Thailand, China, Japan are among the top 15 countries hosting child sexual abuse content)
[139] For example, the age threshold of a child is 19 years old in the Province of British Columbia of Canada, according to the Child, Family and Community Service Act [RSBC 1996] CHAPTER 46, Part 1, 1 (1).

pornographic and obscene/indecent materials are referred to child sexual abuse content and may help.[140] Therefore, in the countries that have no explicit definition of child sexual abuse content, it may be difficult to determine with sufficient certainty whether a given image should be considered potentially illegal child sexual abuse content or not. For an international takedown notice to be issued, the image of a child that is deemed illegal in one country may be legal in another country and the takedown of such a image may not be possible. Take pseudo-photographic images for example, pseudo-photographs are deemed illegal by UK law, no matter whether the images are "made by computer-graphics or otherwise howsoever, which appears to be a photograph". In the US, however, it is legal to create or possess pornographic images of children by means of computers. In *Ashcroft v. Free Speech Coalition*,[141] the Supreme Court held that given that no real children were involved in creating this kind of image, it was unconstitutional to ban it under the Child Pornography Prevention Act of 1996.

In addition, differences exist between potentially criminal activities in relation to child sexual abuse content in various countries. For instance, simple possession of child sexual abuse content (regardless of the intent to distribute) is deemed illegal in 55 of 187 Interpol Member countries, such as, in Australia, Brazil, Germany, Spain, the UK, and the U.S.. The other 132 countries, however, do not criminalise the possession of images of child sexual abuse.[142] Whereas viewing child sexual abuse content from websites without downloading or storing such content is not criminalised as "possession of" or "procuring" such content in many countries, some countries, such as Finland and Slovakia, do penalize such an act.[143] In addition, many countries have no law addressing computer-facilitated child sexual abuse content related offences and such offences are therefore not criminalised in their jurisdictions. Differences between potentially criminal activities in relation to child sexual abuse content could impede international co-operation in tackling child sexual abuse content related crimes across borders, because law enforcement agencies in a country that lacks legislation against, e.g., the possession of child sexual abuse content, may not commit to the seizure of such content, and work to identify child victims or advance the investigations of other countries into online child sexual abuse.

Furthermore, provisions regarding legal responsibility of ISPs vary across countries. In the U.S. and Australia, ISPs are obliged to report sites containing child sexual

[140] For instance, in the UK, the Sentencing Guidelines Council's Definitive Guidelines of the Sexual Offences Act 2003 can help to determine whether a given image should be considered as illegal child pornography.
[141] See Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002).
[142] See *supra* note 4, pp. 17-18.
[143] See *supra* note 4, p.12.

abuse content to the police within a reasonable period of time. Most national legislation does not require ISPs or other service providers to report the detection of sites involving child sexual abuse content on their networks or to preserve records of child sexual abuse content they suspect as evidence for police investigations and legal proceedings.[144] However, the removal of the content may be required once ISPs obtain knowledge of the existence of such content. Differing legal responsibility of ISPs may result in that ISP being notified of child sexual abuse content and acting differently depending on the extent of their legal responsibility.

Legislation is the starting point to address child sexual abuse content related offences on the internet. If legislation on child sexual abuse content related offences is absent, a vacuum that exposes children to the risk of abuse is created. Whilst national legislation exists and covers the problem to varying degrees, different national standards can result in discrepancies in outcomes for offences which are essentially the same at the international level and can create opportunities for those offenders to choose residing in the countries where there is a lower risk of prosecution and lower penalties.

To minimise the negative impact of legislative differences on the efforts against internet child sexual abuse content and provide a holistic legislative framework for international cooperation, two international conventions have been issued to address the multi-jurisdictional problem and to standardise definitions and measures relating to child sexual abuse content related offences. For example, definition of a child as a human being below the age of 18 years is given by the 1989 United Nations Convention on the Rights of the Child. State Parties are also required to take all appropriate national, bilateral and multilateral measures to protect the child from all form of sexual exploitation and sexual abuse. As the main international legal instrument that addresses child sexual abuse content, 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 provides an explicit definition of child sexual abuse content (child pornography) as "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".

Article 3(1) of the Optional Protocol creates obligation on State Parties to criminalise production, distribution, dissemination, importing, exporting, offering, selling or possession of child sexual abuse content, whether committed domestically or

[144] See *supra* note 4, p.13.

internationally or on an individual or organized basis as well as to criminalise simple possession regardless of the intent to distribute. State Parties are also encouraged to establish liability of legal persons for offences specific to child sexual abuse content and to promote international co-operation across borders. In addition, the Council of Europe Convention on Cybercrime that was open for signature and accession by both European states and non-European states also serves the same purpose. The Convention provides definition of the terms of a minor, child sexual abuse content, sexually explicit conduct as well as recommending criminalisation of several forms of child sexual abuse content related offences. The Convention also addresses corporate liability for child sexual abuse content and the importance of international co-operation on cybercrime. However, the drawback of the Convention is that it contains several optional aspects. The Convention sets the age limit at 18, but allows that "a party may, however, require a lower age-limit, which shall not be lower than 16 years", which may result in an age of majority of 16 for the subjects of child sexual abuse content in certain jurisdictions. Simple possession needs not be made a crime while the final clause of Article 9 of the Convention allows that "each party may reserve the right not to apply, in whole or in part" the procurement or possession of child sexual abuse content, which may result in a variety of outcomes for investigations across borders. In addition, computer-generated material is not included by the term of "child pornography" and therefore it may be accepted no matter how realistic the image representing a minor engaged in sexually explicit conduct.

At the regional level, apart from the 2001 Council of Europe Convention on Cybercrime, the 2007 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse is the most recent legal instrument aimed at combating child sexual exploitation, including child sexual abuse content related offences. In the Convention, the term of the age of a child has been clearly defined as "any person under the age of 18 years". A definition of the term "child pornography", similar to that in 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, is also given. The State Parties are required to criminalize production, offering or making available, distribution and transmission, procurement, possession of child sexual abuse content and knowingly obtaining access to such content. The Convention provides clear common standards and definitions on child exploitation and child abuse at the European level at large. However, opt-out provisions, in particular, with respect to production and possession of pornographic material and knowingly obtaining access to child sexual abuse content in the

Convention may again create problems for those tackling online sexual abuse offences across jurisdictions.

All in all, notwithstanding such differences in legislation, there is a general international consensus regarding the seriousness of child sexual abuse content and the sheer size of the problem across the globe. In addition, the UN international conventions provide a holistic and uniform international legal standard for national legislation to be harmonised. If 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 were to be adopted by every country, equivalent legislation in all jurisdictions will surely offer enhanced protection to children worldwide. In so doing, an international notice and takedown system can be effectively developed and implemented against circulation of child sexual abuse content across borders.

4.3.2 Differing Legal Procedures relating to Takedown of Child Sexual Abuse Content

Differences in legal procedures relating to takedown of child sexual abuse content could be another obstacle to the proliferation of child sexual abuse content on the internet and therefore it should be considered if an international notice and takedown system were to be further developed.

Taking the countries which participated in our survey questionnaire for example, legal procedure in relation to notice and takedown of child sexual abuse content varies from one country to another. In the U.S., there is no legal procedure for taking down child sexual abuse content. Electronic Service providers (ESPs) are not required by law to remove or block content, despite these registered ESPs being mandated to report images of child sexual abuse hosted through their services to the CyberTipline. In most cases, ESPs voluntarily remove the content after reporting to the CyberTipline. However, it is lawful for ESPs not to take down the content until they are informed by the law enforcement body that the content they host constitutes child sexual abuse content and should be removed.

Different to their U.S. counterpart, the UK, Germany, and Spain implemented the European Directive on Electronic Commerce into their laws and set out ISPs obligations in relation to online illegal content. Nevertheless, the laws of these three countries do not provide any statutory notice and takedown procedure for the removal of illegal internet content except obliging ISPs to remove or disable access to the content if they have actual knowledge or awareness of the availability of such illegal content. Therefore, in the context of child sexual abuse content, the notice and

takedown procedure is voluntarily implemented under self-regulatory rules and codes of conduct on combating child sexual abuse content over the internet in the UK, Germany, and Spain.

In Brazil, legislation sets out takedown obligations for ISPs by stating that a person is legally responsible for providing the service after being officially notified the existence of illegal content but failing to disable access to it. However, the law does not define the meaning of "official notices" and the body that can issue such notices. In addition, the time frame is not given by the law. Hence, the notice and takedown procedure is in fact instituted in the voluntary agreement between relevant parties, such as, the MoU between the SaferNet Brazil hotline and Google Brazil Internet Limited[145].

In Taiwan, the Internet Content Rating Regulation creates an obligation for internet service providers to restrict access to illegal or banned material or take them down if they have been notified by government agencies or other commissioned bodies of the existence of unlawful content on their network. Therefore, only the law enforcement body or other commissioned bodies such as the ECPAT Taiwan (Internet Safety Hotline web547) can issue authoritative notices to ISPs for the removal of illegal internet content.

The notice and takedown procedure is different in Thailand. According to the Thai law, ISPs are not obliged to take down or block any content except upon authorization of a court order. As a result, for the report concerning child sexual abuse content, only the Thai police or the Ministry of Information and Communication Technology (MICT) can ask a court order to issue notices to ISPs in order to delete or block the content concerned.

Among those that responded our survey, the only country that has clear legal procedures for taking down child sexual abuse content is Australia. Schedule 7 of the Broadcasting Services Act 1992 sets out detailed procedures for taking down prohibited content, including child sexual abuse content that is refused classification. Such a procedure provides details regarding the body that has authority to issue notices, the criteria of determining the illegality of prohibited content, the timescale for complying the notices as well as the penalty of failing to comply with the law. Under Clause 47(1), if the ACMA is satisfied that content is prohibited, having been refused classification by the Classification Board, and the hosting service has an

[145] See Terms of Co-operation between the SaferNet Brazil Hotline and Google Brazil Internet Limited, available at: http://ec.europa.eu/information_society/activities/sip/docs/pub_consult_age_rating_sns/results/safernet_a533690.pdf (last visited on 25 November, 2010)

Australian connection, the ACMA must give the hosting service provider a written notice (final takedown notice) to remove the content. If the content is yet to be classified by the Board, the ACMA must issue an interim takedown notice, after which it must apply to the Classification Board for classification of the content, under Clause 47(2). The ISP must comply with the takedown notice by 6pm the following day or face serious penalties. ISPs are also required under national criminal legislation to notify law enforcement, if they are aware that they are hosting child sexual abuse material.

Other countries such as the UK, Germany, and Spain do not have a statutory notice and takedown procedure. Such a procedure is established through self-regulatory rules and codes of conduct, typically through agreements between hotlines (regardless of the legal status of the hotline) and ISPs. This self-regulatory notice and takedown system brings out an advantage in quick reaction, which is vital for the expeditious removal of child sexual abuse content, because the procedure is not restricted by any specific law and there are usually guidelines to be followed. The hotline can notify the existence of child sexual abuse content promptly for taking down content as long as the national law does not prevent the hotline from issuing takedown notices to ISPs or the police do not specifically request the hotline to do so. An agreement might be reached between the hotlines and the police on a standard operating procedure for notice and takedown in order to avoid hampering the law enforcement investigation and to help hotlines process reports and notices quickly. Disadvantages of non-statutory notice and takedown procedure are however that notices issued by the hotlines, in particular, non-statutory mandated hotline, have no legal standing unless they have been ratified by the law enforcement bodies and so are potentially controversial and may be difficult to be recognised and implemented. As for the development of an international notice and takedown system, it would, however, be easier for the countries that do not have a statutory notice and takedown procedure to exchange intelligence and agree on a procedure for notice and takedown, in particular, on a procedure for taking down content identified by an overseas hotline.

For an international notice and takedown procedure to be implemented in the countries in which ISPs only comply with notices issued by the official bodies, consideration should be given to ensure that the procedures carried out are in accordance with applicable law of these countries and that due deference is given to any law enforcement activities in these country.

While there are countries that have statutory or non-statutory notice and takedown procedures, there are also countries that do not have a law addressing child sexual abuse content and relevant legal procedures. Child sexual abuse content may be taken down by their authorities upon their knowledge or awareness due to their moral and social responsibilities. However, the speed of taking down child sexual abuse content is expected to be even slower in these countries because no specific law and guidelines are to be followed. For an international notice and takedown procedure to be implemented in these countries, legislation is the first priority. Without legislation addressing the issue, no action can be taken against such an increasing crime across borders. Even if an international notice and takedown procedure is further developed, it cannot be implemented in such a country that does not criminalise child sexual abuse related offences.

Due to the fact that variations in national legal procedures relating to notice and takedown of child sexual abuse content may affect the responses to child sexual abuse content and related offences, it is imperative to provide a consistent and comprehensive international standard for taking down child sexual abuse content, in particular, when it may be difficult to require every country's law to set out a statutory notice and takedown procedure. To this end, guidelines on notice and takedown should be developed at the international level, to be adapted and implemented within each country. Multilateral agreements between countries could also be of help while several particular countries may want to provide protocols for the management, in an expeditious manner, of reports from each other with due deference to any law enforcement activities in their jurisdictions.

For the standardised procedure on notice and takedown to be implemented, it would be ideal for every country to have a contact point for the exchange of takedown notices, either within a hotline or within the law enforcement body. While the contact point is set up within a hotline, it is crucial that the hotline establishes a relationship with the local law enforcement body so that intelligence can be passed to the law enforcement body prior to the issuance of takedown notices to ISPs or hosting providers.

4.3.3 Impact on the Complex Network of Relationships on which International Co-operation Relies

In the effort to eradicate online child sexual abuse content, international co-operation has been a crucial element as only whilst there is an established network of relationships in this field, takedown of child sexual abuse content across borders can

be possible. However, this does not necessarily mean that such a network of relationships has been at its most effective in ensuring that child sexual abuse content is taken down across the globe. While variation in national laws, legal procedure relating to child sexual abuse content and operational procedures of the organisation issuing takedown notices remain, further development of a notice and takedown system at an international level and its implementation may have an impact on the complex network of relationships on which international co-operation relies.

Differences between national laws suggest that some takedown notices may be actionable in one country but may not be in another country. If a hotline in the U.S. or in the UK detects such an image of someone appearing to be 19 hosted by an ISP in their internet territory, they would not issue takedown notices and the ISP would not be required to act upon it. However, notice regarding the removal of such an image is certainly actionable in the province of British Columbia of Canada due to the fact that the age threshold of a child is 19 years old in the law. The discussion on the differences of the law regarding pseudo-photographic images in the U.S. and the UK[146] also demonstrates the significance of the criterion of content that justifies issuing an international takedown notice. Therefore, it is crucial to understand what constitutes content that justifies issuing a notice because failure to respond to an international takedown notice could damage confidence and trust built up between hotlines. However, it would be understandable if no action being taken was because of the variation in national legislations. Yet, it is of vital importance to standardise what would constitute requiring an international takedown notice being sent in order to save the time and cost of the hotlines to make their work more efficient and to avoid damaging working relations between hotlines.

Issuing takedown notices directly to an international ISP may affect the complex network of relationships on which international co-operation relies, in particular, when the issuing of international notices bypasses the hotline within the country where the ISP is based and where working relationships between the hotline and local law enforcement body as well as domestic ISPs may be well-established. The existence of a hotline in a country has its reason and the work of the hotline serves certain purposes. The hotline establishes operational procedure and cooperates closely with domestic ISPs to help keep their services free from illegal content and to protect their staff from having to deal with issues relating to illegal content without suitable training and counselling. If an outside hotline issues takedown notices

[146] See page 95, para 1 of this Report ("Take pseudo-photographic images for example, pseudo-photographs are deemed illegal by the UK law ……")

directly to a foreign ISP, the usual routine of the ISP for dealing with issues relating to child sexual abuse content will be interrupted because they may only be required to act upon notices by the police or other authoritative organisations such as hotlines of their country. Hence, a notice issued by a foreign hotline may confuse the ISP regarding how they should respond and whether the content identified by the hotline of another jurisdiction is actually illegal and should be taken down pursuant to the domestic law. When an ISP does not have the resources (e.g. trained analysts with sound knowledge of relevant law) which a hotline has to assess the legality of the reported content, the removal of such content may result in wrongful takedown of legitimate content and hence undermine freedom of expression.

A similar impact will occur when the law enforcement body is not informed in a country that the content is hosted and where a hotline does not exist. Currently, advisory takedown notices for content hosted abroad are sent via local law enforcement agencies of the hotline and then Interpol so that the relevant law enforcement agencies are alerted about the existence of the child sexual abuse content and a possible child sexual abuse crime behind the content. If a hotline issues a notice directly to an overseas ISP and the ISP takes down identified content without keeping law enforcement informed, relevant intelligence and evidence may not be collected and preserved as required for investigation and ongoing surveillance may be disrupted, as a result, law enforcement bodies' efforts to combat child sexual abuse content related crimes in a particular country will be compromised.

To ensure an international notice and takedown procedure is further developed and effectively implemented without affecting the complex network of relationships on which international co-operation relies, it would be desirable to have in place a global agreement on what constitutes content that justifies issuing a takedown notice. In addition, international agreement needs to be reached to ensure that consistent international takedown procedures work through the local hotline and law enforcement agencies in each case so that a local point of contact for any appeal/review action that ISPs or content owners wish to take is provided and law enforcement activities are not compromised.

4.3.4 Specific Impact on Law Enforcement Activity relating to Child Sexual Abuse Content related Offences

As discussed in Part 3 of the report, the law enforcement activity and an international notice and takedown system relating to child sexual abuse content have different priorities, although they share the same common goal of combating online

child sexual abuse content. Whilst the international notice and takedown system aims to remove child sexual abuse content in the most timely manner, this may interfere with law enforcement activity if the issuance of takedown notices bypasses the relevant law enforcement establishment. For example, when legally permitted, the hotline in one country may issue takedown notices directly to overseas ISPs. While the law enforcement body in the corresponding country where the content is physically hosted is not informed, or that the ISP who received the takedown notice does not report the existence of such content to the local law enforcement body, law enforcement investigation of the correspondent country may be jeopardized and ongoing surveillance activity may be disrupted. In addition, forensic data as evidence in particular cases may be lost due to that the ISP deleting such content without realising that the content is actually the subject of a police investigation and therefore should be preserved as evidence.

Another possible scenario which may impede foreign law enforcement activities is where a working relationship between the law enforcement body and the hotline has not been established, by implementing an international notice and takedown system, the hotline may, without informing the local law enforcement, direct ISPs to expeditiously remove child sexual abuse content notified by their partner hotlines in other jurisdictions. In this case, due to the lack of communication with the law enforcement agency, the hotline will not be able to verify whether the law enforcement agency is actively investigating the website or any individuals associated to the content being removed. As a result, the issuance of notices may interrupt law enforcement activity.

To effectively implement an international notice and takedown system while in the meantime minimising its negative impact on investigation by foreign law enforcement agencies, it is better for the hotline that has identified potentially criminal child sexual abuse content hosted in other jurisdictions to issue advisory notices regarding the existence of child sexual abuse content, rather than issue notices for takedown because as a hotline outside of a specific jurisdiction they will not be able to verify the applicable law in the country of origin. Hence, the takedown decision should be made by the hotline or ISPs who received the advisory notices after consulting the local law enforcement agencies based on their domestic laws and legal procedures.

Another way to minimise the impact of an international notice and takedown system on law enforcement activities in relation to child sexual abuse content is to encourage the hotline to develop good working relations with their law enforcement agencies. When a good partnership is formed between the law enforcement body and the

hotline, the hotline may establish regular contact with the law enforcement body in order to inform them of the existence of child sexual abuse content identified prior to taking any possible action. The hotline may also be updated by the law enforcement body if there are ongoing investigations concerning the content identified, and if takedown notices are necessary or should be postponed. Further agreement should include a timescale for the police to react, after which the hotline would proceed with giving notice.

A well-developed international notice and takedown system should not affect law enforcement activity but can bring in benefits in a numbers of ways. Key benefit being that while the hotlines operating a notice and takedown system not only provide a reporting point for the public to report potentially criminal child sexual abuse content, they also identify, assess and trace child sexual abuse content. The statistic provided by the Spanish Protegeles hotline is the best illustration of such a value added to the law enforcement body. According to Protegeles, 5,113 out of 28,992 reports received by the hotline were referred to the law enforcement agency after more than one year's work of several content analysts, while the remaining 23,879 were not considered to be illegal. By assessing all the reports and singling out the potentially criminal content, the hotline saved the time and effort of the law enforcement agency to receive and check through all the content contained in 28,992 reports.[147] Therefore, the notice and takedown system operated by the hotlines as well as the network of international hotlines could significantly reduce the workload on national law enforcement agencies and prevent them from being inundated with reports of child sexual abuse content which is hosted in and/or outside their jurisdiction. This is significant in particular when law enforcement budgets are tight and they may not be able to devote necessary resources to deal with the reports quickly. Secondly, critical evidence for child sexual abuse content related crimes can be preserved through a well-developed international notice and takedown procedure operated by hotlines. For example, in a country that has a hotline, there is usually a working partnership between the hotline and their domestic ISPs, either mandated by the law or formed voluntarily. [148] Within the framework of such a partnership, the ISPs are usually required to remove or block access to potentially criminal child sexual abuse content identified but at the same time to ensure all relevant evidence preserved for further law enforcement investigation and prosecution.

[147] See *supra* note 121.
[148] To be an INHOPE hotline this is a requirement, but in countries such as Brazil and China, which are currently not members of INHOPE, the working partnership is established through voluntarily agreement.

The requirement to preserve potentially criminal child sexual abuse content for investigation is reflected in the agreements between the hotlines and ISPs in countries where a notice and takedown procedure is well-developed. In addition, by operating a notice and takedown procedure, the hotline themselves can assist law enforcement activity by providing statements of evidence to support law enforcement investigations. This has been done in the UK by the IWF and this is the reason that the IWF Hotline has received very positive feedback from a number of law enforcement agencies across the country over the years. In the U.S., content analysts of the CyberTipline have also been providing direct technical assistance and research for ongoing investigations at the request of law enforcement.

Another value added is the training provided by some hotlines to their law enforcement partners although this may not be the case in all the countries. In order to better operate a notice and takedown system and work effectively with their police partners in combating child sexual abuse content, some hotlines not only train their content analysts and provide psychological support to those who look at traumatic child sexual abuse content in the course of their work, they also help to train national and local law enforcement officers about issues of children and online technologies such as tracing illegal content as indicated by the UK IWF hotline, the Spanish Protegeles hotline and the Brazilian SafeNet hotline. This again will save the law enforcement effort in training their officers on the issues regarding internet technologies particularly relating to the production and distribution of child sexual abuse content, and/or enhance their knowledge on these issues if similar training has already been provided within the law enforcement agencies.

In order to benefit law enforcement activity from an international notice and takedown system as well as to make an international notice and takedown system more effective, it is of paramount importance to develop a sound working relationship with the law enforcement body. The experiences of the hotlines in the UK, Spain, Brazil, the U.S. and Germany have provided good examples for other hotlines to follow. INHOPE has also provided best practice policies regarding notice and takedown procedure in which the essential communication and preferred working relationship between the hotline and law enforcement agency are outlined. In addition, provisions in the EU European Commission Guidelines for Co-funded Hotlines on Notice and Takedown can be helpful for those that have not formed a close partnership with their law enforcement agencies. It is suggested in the second version of the drafted guidelines that hotlines should not notify the existence of the illegal content to the host service provider if national law prevents them from doing

so or they are specifically requested not to do so by the police. Hotlines should do their outmost to reach agreement with the police on a standard operating procedure for notice and takedown, which provides for the hotline to inform the police about the content identified, the host service provider and the country where the content is hosted. The agreement should preferably stipulate a deadline for the police to react after which the hotline would proceed with giving notice. Ideally, the hotline has an operational procedure endorsed and supported by law enforcement agency.[149]

Guidelines[150] adopted by the Global Conference "Co-operation against Cybercrime" in 2008 for the co-operation between law enforcement and internet service providers against cybercrime could also be of help to engage law enforcement agencies and ISPs to tackle child sexual abuse content. It is important for the implementation of an international notice and takedown system in a country that does not have a hotline that the ISPs that received advisory notices regarding the existence of potentially illegal child sexual abuse content consult local law enforcement authorities for appropriate action towards the reported content.

4.3.5 Risks to an Organisation of Issuing International Takedown Notices

When an organisation issues takedown notices for the removal of child sexual abuse content, risks includes legal challenge, risk of reputation of the organisation as well as the risk of compromising law enforcement activity. Hence, it is very likely that the issuing of international takedown notices will also generate risks to the organisation that issues takedown notices at an international level if relevant issues with respect to such an organisation are not clarified in an international notice and takedown system.

Legitimacy of the organisation issuing takedown notices to access reported illegal content containing child sexual abuse content could be a central issue causing controversy. According to the overview of INHOPE regarding legal rights and permission for INHOPE civil hotlines to access reported illegal content containing child sexual abuse images, there are 16 out of 31 INHOPE countries' hotlines which have no legal rights to access reported illegal content containing child sexual abuse content. Despite this they have been doing so since their establishment. Arguably, some of them have had agreements with their law enforcement bodies and their law

[149] See "European Commission Guidelines for Co-Funded Hotlines on Notice and Take-down" (v4 28.9.10), 3. Relations with the Police
[150] See "Guidelines for the Co-operation between Law Enforcement and Internet Service Providers against Cybercrime", available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567_prov-d-guidelines_provisional2_3April2008_en.pdf (last visited on 10 November 2010)

enforcement agencies have authorised them to access and monitor child sexual abuse content. It was indicated from the responses of the hotlines to our survey that the hotlines have never been challenged for the issuance of takedown notice for the removal of child sexual abuse content due to the legitimacy of their access to the reported child sexual abuse content. However, the role of hotlines in dealing with child sexual abuse content over the internet might still be questioned. In the UK, the Department of Trade & Industry and the Home Office reviewed the structure and work of the IWF in 1998 and encouraged the clarification of the role of the IWF in relation to relevant material on the internet after the role of the IWF was questioned by the UK free speech organisation Cyber-Rights and Cyber-Liberties[151]. Hotlines such as the IWF will contend that they have been recognised as a relevant authority for reporting, assessing and judging child sexual abuse images on behalf of their law enforcement agencies,[152] and the work of the hotlines has been supported by their government as well as funded by the European Union over the years. It would still be desirable that hotlines have a clear legislative basis for accessing and examining child sexual abuse content.

In addition, legitimacy of issuing takedown notices to overseas ISPs is also an issue that should be considered in the development of an international internet notice and takedown system because it could bring risks to the organisation if not addressed. This is particularly important to those "notice and takedown" bodies that are some form of public authority.

Another risk is to the reputation of the organisation, which may be caused by lack of transparency and accountability of the hotline procedures. For example, without conducting a proper contextual assessment, perception on the age of a child or legality of the image may be wrongly formed due to the complication added by social and cultural differences. An incorrect notice may be sent to ISPs while a quality assurance process is not established and strictly followed in order to ensure that the reported child sexual abuse content are correctly assessed in accordance with the law. The lack of standardised procedures may therefore lead to the removal of legitimate content and therefore jeopardise freedom of expression and public access to information. It may also provoke litigation against the organisation that issued such a notice where the organisation may be responsible for liability. The lack of detailed

[151] See Yaman Akdeniz, Internet Child Pornography and the Law, Aldershot, England: Ashgate, 2008, pp.264-266.
[152] See for example, in the UK, the role of the IWF relating to child sexual abuse content has been recognised in a "Memorandum of Understanding between the Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) linked to Section 46 of the Sexual Offences Act 2003", available at: http://www.iwf.org.uk/assets/media/hotline/SOA2003_mou_final_oct_2004.pdf (last visited on 16 November 2010)

guidance on how to remove identified child sexual abuse content while preserving evidence for police investigations may also result in the loss of forensic data as evidence because some ISPs may not know the technique necessary for removing child sexual abuse content or disabling the public's access to particular content without compromising evidence preservation for law enforcement investigation.[153]

While organisations that issue takedown notices are supported by government, law enforcement body, the online industry and majority of internet users in the countries of operation, public trust and confidence remain important. Hence, it is imperative for the organisations to build a good reputation for the work and success of the organisations [154] and to develop and maintain high operational standards on, management of the reports, identification, assessment and tracing of child sexual abuse content, issuance of notices, assistance to the ISPs for taking down content as well as for preserving evidence for law enforcement investigation, and processes for complaints.

Apart from the legal and reputation risks, the most significant risk is to compromise a police investigation if the issuing of takedown notices bypasses law enforcement. When notices for removing child sexual abuse content are issued directly to ISPs without informing relevant law enforcement agencies, it means that specific law enforcement investigation of the home country or the correspondent country may be jeopardized and ongoing surveillance activity may be disrupted. Potentially, this could have a negative impact on the relationship between the organisation that issues takedown notices and the law enforcement bodies. The support of the law enforcement agencies is vital to the work of the organisation that issues takedown notices, therefore compromising law enforcement activity could not only generate a significant risk to the success of the organisation, but could also undermine the efforts in bring those responsible for distribution of child sexual abuse content to justice.

4.4 Conclusion

Whilst the findings of the research suggests that the potential for further developing an international notice and takedown system is significant, there are five identified challenges including

[153] So far, as the author is aware, that only the IWF provides a best practice guide for Systems Administrators on how to preserve data but remove public access.
[154] As the author is aware, that the UK IWF is fully transparent and are independently audited every three years.

- challenges posed by differing national legal standards relating to child sexual abuse content;
- challenges posed by differing legal procedure relating to the takedown of such content;
- impact of the development of an international notice and takedown system on the complex network of relationships on which international co-operation relies;
- impact of such an international notice and takedown system on the activities of law enforcement bodies
- the risks to a national hotline organisation issuing international takedown notices.

The influential factors are not exhaustively explored in this research, but the discussion in the report serves as a view point from which to contemplate how a global notice and takedown system can be further developed and effectively implemented in order to achieve the expeditious removal of internet child sexual abuse content at an international level.

The implications of the research are that variations in national law and legal procedures do have an impact on further development and effective implementation of an international notice and takedown system in relation to child sexual abuse content. Differences in relation to definitions of child sexual abuse content, potentially criminal activities and legal responsibility of ISPs may also have impact on the effective development and implementation of such an international notice and takedown system. The standard and effectiveness of legal procedures relating to the removal of child sexual abuse content is also diverse across the global. Nevertheless, a general international consensus regarding the seriousness of child sexual abuse content has been reached among countries, therefore, there are possibilities for national legislation to be harmonised, in particular, when UN international conventions have provided a holistic and uniform international legal standard for national legislation to be harmonised. It is also possible to develop guidelines on notice and takedown in relation to child sexual abuse content at an international level in order to make implementation of an international notice and takedown system more effective.

While variations in national law and legal procedures may be the central issues for the further development and implementation of an international notice and takedown system, several other factors cannot be ignored because they may also affect the further development and implementation of an international notice and takedown

system. Nevertheless, the impact of an international notice and takedown system on the level of international co-operation can be minimised by international efforts towards a global agreement. Developing and maintaining a close working partnership between the law enforcement body and the organisations issuing takedown notices can curtail the impact of such a system on law enforcement activity. As long as potential risks faced by the organisations issuing takedown notices are identified and addressed, it would not impede the hotlines to issue takedown notices internationally.

Part 5: Conclusion and Recommendations

The availability and distribution of child sexual abuse content continues to raise concerns for society and a notice and takedown system is one element in a distributed enforcement regime for combating child sexual abuse content on the internet, which would also include statutory regulation, internet blocking and other disruptive tactics.

This research examines further development and effective implementation of an international notice and takedown system. An international notice and takedown service has already been established in a number of countries such as the UK, the U.S., Germany, Spain, Australia and Taiwan within the network of INHOPE as well as in other countries such as Brazil, Thailand, and China. Despite the existing international notice and takedown service adopted in a number of countries helping to provide a mechanism for receiving complaints from the public, collecting intelligence for law enforcement, removing child sexual abuse content from servers, and providing protection to children as well as internet users, a great deal of child sexual abuse content still cannot be effectively taken down, in particular, on the internet territory of countries that are not part of the INHOPE network. Whilst online child sexual abuse content is shifting and re-emerging with assistance of new technologies to meet continuous demand for such content over the internet, the capability of the individual hotlines and the INHOPE network is limited to minimising the circulation of child sexual abuse content worldwide, and therefore the need of a further developed and comprehensive international notice and takedown system relating to child sexual abuse content.

The study conducted a cross sectional study on notice and takedown practices from various countries around the globe and discussed the pros and cons of the existing regulatory regimes relating to child sexual abuse content. These include statutory regulation, internet blocking and a notice and takedown system. The research suggests that there is a consensus among countries that an international notice and takedown system is part of a multifaceted approach to reduce the availability of child sexual abuse content, and a more co-ordinated effort is needed to enhance such a notice and takedown system in order to frustrate access to child sexual abuse content. The potential for further developing and implementing an international notice and takedown system is investigated and several issues that might have an impact on further development and effective implementation of such a notice and takedown system at the international level are identified. Inconsistent legislation in all jurisdictions regarding child sexual abuse content and related offences and

differing legal procedure for the removal of such content are the two main obstacles to be overcome. In addition, the impact of an international notice and takedown system on law enforcement activities and a complex network of relationships between the organisations that issue international takedown notices are also vital. This requires that such an international notice and takedown system comprehensively addresses relevant issues to support the police investigation and co-operation of the hotlines. Risks relating to an organisation that issues international takedown notices, if not addressed and mitigated, will damage confidence of the organisation in engaging in the battle against child sexual abuse content.

To further develop an international notice and takedown system and implement such a system on a more broad scale to prevent and eradicate child sexual abuse content and prevent the internet and new technologies from being used for the circulation of such content, the report recommends:

1. To minimise the impact of different national standards on the further development and effective implementation of an international notice and takedown system, harmonization of laws relating to child sexual abuse content is essential.

- At the international level, it is important to promote the adoption and ratification of the two UN international Conventions: the 1989 United Nations Convention on the Rights of the Child and 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, both of which provide legal basis for national legislation relating to child sexual abuse related offences.
- At the regional level, and in particular within the EU, it is vital for the EU to update their existing policies and legal instruments relating to child sexual abuse content to ensure that the diverse legislation of the Member States are harmonised under a coherent and holistic legislative framework. This might include, to criminalise new forms of child sexual abuse offences using information technology, to include simple possession and procurement of child sexual abuse content; to define computer-generated child sexual abuse materials as one of the forms of child sexual abuse content. This is particularly important for the swift removal of child sexual abuse content at source within the European internet territory, as currently EU is still a region that hosts a considerable amount of child sexual abuse content.
- National legislation in line with the international convention helps to create a sound legal basis for international cooperation, particularly in terms of further

development and implementation of a notice and takedown system at an international level. At the national level, governments around the world should adopt clear, comprehensive, and holistic legislation to protect children from child sexual abuse internet related crimes. For so doing, it is needed

- to make it clear in the relevant legislation that child sexual abuse content offences are a serious violation of the rights of children;
- to standardise the terms of age of a child and age of consent;
- to standardise the definition of child sexual abuse content including virtual photographs or pseudo photographs;
- to criminalize all aspects of online child sexual abuse – the production, distribution, dissemination, importing, exporting, offering, selling or possession of child sexual abuse content as defined in Article 3(1) of 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;
- to define new criminal offences facilitated by the use of IT such as, simple possession of child sexual abuse content, knowingly obtaining access to child sexual abuse content including viewing such content from websites without downloading or storing the content.
- to clarify responsibilities of internet service providers and other stakeholders in this regard.

2. To mitigate the impact of differing legal procedures relating to the removal of child sexual abuse content on the further development and effective implementation of an international notice and takedown system, it is important to develop a consistent and comprehensive international procedure for taking down child sexual abuse content, with due deference to applicable domestic laws. Such an international standard should be adapted and implemented within each country in order to benefit international co-operation from harmonization of procedures while there are no borders between countries for internet users. Multilateral agreements between countries should also be encouraged while some particular countries may want to provide protocols for the management, in an expeditious manner, of reports of child sexual abuse content from each other with due deference to any law enforcement activities in their jurisdictions.

3. To maintain and enhance the complex network of relationships on which international co-operation relies in the development and implementation of an international notice and takedown system, harmonization of practice and procedures

between the organisations that issue international takedown notices is required, in particular, relating to standards of what would constitute requiring an international notice being sent, access to and exchange of information regarding child sexual abuse content as well as operational procedures for the co-operation between the hotlines and law enforcement bodies as well as ISPs. Best Practice Guidelines of INHOPE on Notice and Takedown Procedures, European Commission Guidelines for Co-Funded Hotlines on Notice and Takedown are two good examples that can be reviewed and enhanced going forward.

4. It is suggested in the discussion of Part 4 that the minimization of the impact of an international notice and takedown system on the law enforcement activity relating to child sexual abuse content depends on how effective the working relations between the hotlines and the law enforcement bodies are. Therefore, a recommendation in this aspect is to encourage the development of a good partnership between the hotlines and the law enforcement agencies. Where a closer working partnership has not been established, it is still vital that an international takedown notice is sent without bypassing the law enforcement route such as via domestic law enforcement body or Interpol, Europol so that possible law enforcement activities are not compromised.

5. To minimise or provide cover for the risks to the organisations that issue takedown notices, it is imperative to develop a risk management strategy and to implement such a strategy effectively. Such a strategy should be regularly reviewed and the performance should be monitored. The risk management strategy for an organisation issuing takedown notices includes elements such as

- policies and standards;
- responsibilities and accountability;
- detailed procedures on management of the reports;
- identification, assessment and tracing of child sexual abuse content;
- issuance of notices;
- assistance to the ISPs for taking down content as well as for preserving evidence for law enforcement investigation,
- quality assurance mechanisms, and
- processes for complaints which make their operational standards and polices transparent to members of the public.

Procedures on how to liaise with law enforcement agencies, ISPs and other relevant parties such as the domestic government, sister hotlines in other

jurisdictions, the sponsors as well as other international organisations in this area should also be part of the risk management strategy. In addition, to endeavour for legal clearance is particularly important to an organisation that does not have a clear legislative basis for accessing, examining child sexual abuse content and issuing takedown notices.

Bibliography

Ahlert, Christian, Chris Marsden and Chester Yung, "How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation", retrieved on 13th May 2010 from: http://www.rootsecure.net/content/downloads/pdf/liberty_disappeared_from_cyberspace.pdf

Akdeniz, Yaman, "Internet Child Pornography and the Law" (Aldershot, England: Ashgate, 2008)

……, "To Block or not to Block: European Approaches to Content Regulation, and Implications for Freedom of Expression", Computer Law & Security Review, 26(2010), pp. 260-272

……, "Who Watches the Watchman? The Role of Filtering Software in Internet Content Regulation", retrieved on 22th September 2010 from: http://www.osce.org/item/13570.html?ch=93.

Baines, Victoria, "Online Child Sexual Abuse: The Law Enforcement Response", November 2008, pp.15-16

BBC News, "Delete Child Abuse Websites Says German Minister", 31 March 2010, retrieved on 1st April 2010 from: http://news.bbc.co.uk/1/hi/technology/8596650.stm

Brady, John J., "Banding Together Industry Coalition Combats Child Pornography with a Global, Strategic Focus, Transaction Trends", August 2010

Bunzeluk, Kelly, "Child Sexual Abuse Images: An Analysis of Websites by Cybertip!Ca", November 2009

Byron, Tanya, "Safer Children in a Digital World: The Report of the Byron Review" (London: Department for Children, Schools and Families and Department for Culture, Media and Sport, 2008)

Callanan, Cormac, Marco Gercke, Estelle De Marco, and Hein Dries-Ziekenheiner, "Internet Blocking - Blancing Cybercrime Responses in Democratic Societies", October 2009, retrieved on 17th March 2010 from: http://www.aconite.com/sites/default/files/Internet_Blocking_and_Democracy_Exec_Summary.pdf

CIRCAMP, "How Many Countries are Blocking Child Pornography on the Internet?", retrieved on 20th September 2010 from: http://circamp.eu/index.php?view=items&cid=1%3Ageneral&id=17%3Ahow-many-countries-are-blocking-child-pornography-on-the-internet&option=com_quickfaq&Itemid=9

Clayton, Richard, "Judge & Jury? How "Notice and Take Down" Gives ISPs an Unwanted Role in Applying the Law to the Internet", QuickLinks - Liability, Jurisdiction and Applicable Law, Issue no. 214, 23 November 2001

……, Failures in a Hybrid Content Blocking System. In: George Danezis and David Martin, (Editors): Privacy Enhancing Technologies, Fifth International Workshop, PET 2005, Cavtat, Croatia, May 30-June 1 2005, volume 3856 of LNCS, pp.78-92, Springer Verlag

……., Tyler Moore, The Impact of Incentives on Notice and Take-down, Seventh Annual Workshop on Economics and Information Security (WEIS08), Dartmouth NH, USA, June 25--28 2008. In: M. Eric Johnson, editor: Managing Information Risk and the Economics of Security, pp.199-223, Springer, New York, 2008

Craddock, Peter A., "Legal Implication of Internet Filtering", (LLM Dissertation, University of London, 2010)

Culture, Media and Sport Select Committee of the UK, "Harmful Content on the Internet and in Video Games, 22 July 2008, retrieved on 10th December 2010 from: http://www.publications.parliament.uk/pa/cm200708/cmselect/cmcumeds/353/353.pdf.

Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, editors, "Access Denied: The Practice and Policy of Global Internet Filtering" (London, England: The MIT Press, 2008)

Department for Business, Innovation and Skills, "Digital Britain Final Report", June 2009, retrieved on 14th April 2010 from: www.official-documents.gov.uk/document/cm76/7650/7650.pdf

Eco, "The eco Internet Complaint Hotline Results 2009-2010", August 2010.

Edwards, Lillian, "From Child Porn to China, in One Cleanfeed", SCRIPT-ed, Volume 3, Issue 3, September 2006, PP.174-175

……, "Pornography, Censorship and the Internet", July 16, 2009, retrieved on 13th April 2010 from: http://ssrn.com/abstract=1435093

European Digital Rights, "Deleting Illegal Sites is More Efficient than Blocking them", EDRi-gram - Number 8.17, 8 September 2010

……., "ENDitorial: Internet Blocking in Ten Weeks and Counting", EDRi-gram - Number 8.18, 22 September 2010

European NGO Alliance for Child Safety Online, "Using Blocking to Combat Online Child Abuse Images: Questions and Answers", April 2009, retrieved on 13th April 2010 from: http://www.enacso.eu/index.php?option=com_rokdownloads&view=file&task=download&id=14%3Abriefing-on-blocking-of-online-child-abuse-material&Itemid=11.

European NGO Alliance for Child Safety Online, "Position Paper: Child Sexual Abuse Online and Child Abuse Images", June 2009, retrieved on 20th September 2010 from: http://www.enacso.eu/index.php?option=com_rokdownloads&view=file&task=download&id=15%3Aenacso-position-paper-on-child-sexual-abuse-online-and-child-abuse-images&Itemid=11.

Europol, "Child Sexual Exploitation 2010 Fact Sheet", retrieved on 19th December 2010 from: www.europol.europa.eu/.../Child_sexual_exploitation_factsheet_2010.pdf

Frayssinet, Fabiana, "War against Child Pornography on the Internet", retrieved on 17th July 2010 from: http://ipsnews.net/news.asp?idnews=44906

Gillespie, Alisdair A., "Defining Child Pornography: Challenges for the Law", Child and Family Law Quarterly, 2010, 22(2), pp. 200-222

……, "Regulation of Internet Surveillance", European Human Rights Law Review, 2009, Issue 4, pp. 552-565

……, "Legal Definitions of Child Pornography", Journal of Sexual Aggression, 2010, 16: 1, pp. 19-31

Heins, Marjorie, Christina Cho, and Ariel Feldman, "Internet Filters: A Public Policy Report", 2006, 2nd edition, retrieved on 3rd July 2010 from: http://www.fepproject.org/policyreports/filters2.pdf

Hustinx, Peter, "Opinion of European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on Combating Sexual Abuse, Sexual Exploitation of Children and Child Pornography, Repealing Framework Decision 2004/68/JHA, 10 May 2010

International Centre for Missing & Exploited Children, "Child Pornography: Modern Legislation & Global Review", 2010, 6th Edition

……, "Resolution of the Board of Directors", 15 October 2010, retrieved on 16th October 2010 from: http://www.icmec.org/en_X1/pdf/Blocking_Resolution_EN.pdf

IWF, "IWF Facilitation of the Blocking Initiative", retrieved on 14th May 2010 from: http://www.iwf.org.uk/public/page.148.htm

……., "Combating Online Child Sexual Abuse Content at National and International Levels: IWF Experience, Tactical Suggestions and Wider Considerations", 26 July 2010, retrieved on 26th July 2010 from: http://www.iwf.org.uk/media/page.70.636.htm

……., "2009 Annual and Charity Report", retrieved on 26th November 2010 from: http://www.iwf.org.uk/documents/20100511_iwf_2009_annual_and_charity_report.pdf

Japan Today, "Gov't to Have Internet Providers Block Access to Child Porn Images", 27 July 2010, retrieved on 28th July 2010 from: http://www.japantoday.com/category/national/view/govt-team-oks-plan-to-get-isps-to-block-access-to-child-porn-images

Kleinsteuber, Hans J," The Internet between Regulation and Governance", retrieved on 22th September 2010 from: http://www.osce.org/item/13570.html?ch=93.

Krone, Tony, "International Police Operations against Online Child Pornography, Trends and Issues in Crime and Criminal Justice", April 2005, No. 296, retrieved on

23th May 2010 from: http://www.aic.gov.au/documents/3/C/E/%7B3CED11B0-F3F4-479C-B417-4669506B3886%7Dtandi296.pdf

Kurbalija, Jovan, "An Introduction to Internet Governance" (4th edition, Malta: DiploFoundation, 2010)

Maalla, Najat M'jid, (Special Rapporteur) "Report on the Sale of Children, Child Prostitution and Child Pornography, Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, including the Right to Development", A/HRC/12/23, 13 July 2009, presented at the Twelfth session of the General Assembly of the United Nations

McIlveen, Luke, "No Money Available to Chase Internet Paedophiles", The Daily Telegraph, 18 June 2007

McGlynn, Clare, & Erika Rackley, Criminal Law Review, 2009, 4, pp. 245-260

Muir Deborah, (ECPAT International), "Violence against Children in Cyberspace", 2005, retrieved on 3rd April 2010 from: http://www.ecpat.net/ei/Publications/ICT/Cyberspace_ENG.pdf

Office of Communication of the UK, "Criteria for Prompting effective Co and Self-Regulation", retrieved on 14th April 2010 from: http://stakeholders.ofcom.org.uk/binaries/consultations/co-reg/statement/co_self_reg.pdf.

Ozimek, Jane Fae, "IWF: Good on Child Abuse.....Obscenity, Racism, not So Much", 13th May 2010, retrieved on 13th May 2010 from: http://www.theregister.co.uk/2010/05/13/iwf_2010/

Peguera, Miquel, "I just Know that I (actually) Know Nothing: Actual Knowledge and Other Problems in ISP Liability Case Law in Spain", European Intellectual Property Review, 2008, 30(7), pp.280-285

Petit, Juan Miguel, (Special Rapporteur) "Report of the Commission on the Sale of Children, Child Prostitution and Child Pornography, Rights of the Child", E/CN.4/2005/78, 23 December 2004, presented at the sixty-first session of the General Assembly of the United Nations

Pia Mifsud Bonnici, Jeanne, "Self-Regulation in Cyberspace" (The Hague: TMC Asser Press, 2008)

Ramage, Sally, "Child Abuse in the United Kingdom", Criminal Lawyer, 2009, 191, pp.1-3

Reid, Alan S., "Online Protection of the Child within Europe", International Review of Law Computers & Technology, 2009, 23(3), pp. 217-230

Sara M, Smyth, "Mind the Gap: A New Model for Internet Child Pornography Regulation in Canada", retrieved on 13th November 2010 from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1345910

Steel, Chad M.S., "Child Pornography in Peer-to-Peer Networks", Child Abuse & Neglect, 33, 2009, pp. 560-568

Walden, Ian, "Porn, Pipes and the State: Censoring Internet Content", The Barrister, 13th April 2010

Williams, Chris, "BT Blocks up to 40,000 Child Porn Pages Per Day: Cleanfeed Busy", 7 April 2009, retrieved on 13th April 2010 from: http://www.theregister.co.uk/2009/04/07/bt_cp_figures/ (last visited on 21 September 2010)

Williams, Nigel, "The Contributions of Hotlines to Combating Child Pornography on the Internet", 1999, retrieved on 16th April 2010 from: http://www.childnet-int.org/downloads/combating-child-pornography.pdf

Appendix: Survey Questionnaire

The Development of a Comprehensive, Transferable International Internet Notice and Takedown Best Practice Model Relating to Child Sexual Abuse Content

The Internet Watch Foundation is currently undertaking a research project funded by the Nominet Trust looking into the development of a comprehensive, transferable international notice and takedown best practice model relating to child sexual abuse content.

To conduct the research, we will focus on various countries in more detail to describe what is currently in place for countries with a hotline, without a hotline, those with a hotline that are not a member of INHOPE and to take a cross section of these from various locations around the globe.

We greatly appreciate your response to the questionnaire below and would be very grateful if you can share with us any other materials that would be beneficial to this research.

Survey Questionnaire

I. Legislative regime relating to child sexual abuse content

1. What is the national standard relating to child sexual abuse content in your country, e.g. age threshold? Please provide relevant legal documents where available.
2. Does the law in your jurisdiction require ISPs to take down or block child sexual abuse content?
3. What is the legal procedure relating to takedown of child sexual abuse content in your country?
4. How successful is the notice and takedown procedure in relation to child sexual abuse content in your jurisdiction?

II. Hotline (Notice and Takedown Procedure)

5. Are you the only hotline dealing with child sexual abuse content in your country?
6. Do you train your hotline team regularly to ensure that they are provided sufficient knowledge to judge the illegality of the reported child sexual abuse content? Does the training involve your local law enforcement agency or other legal professions?
7. Does your hotline have a monitoring process to check if the reported content has been taken down? What do you do if the content has not been taken down?
8. Does your hotline provide an appeals process for unblocking legitimate websites/contents that are inadvertently filtered by system in place in your country?

9. Does your hotline have quality assurance process in place, which is a process-driven approach with specific steps to ensure the reported child sexual abuse content are correctly assessed in accordance with the law?
10. Have your hotline ever been challenged for the issuance of a notice requiring ISPs to remove child sexual abuse content? If yes, who challenged your activities: the ISP, the users or the law enforcement agency?
11. Have your hotline ever issued advisory notices to international service providers in another countries and what was their reaction?
12. If your hotline does not have much contact with overseas law enforcement, will you pass the reports onto your local law enforcement agency so that they can get in touch with law enforcement body in another country in order for the reported child sexual abuse content to be removed, or, you will simply block the access to those contents?
13. What would be the negative impact on the removal of child sexual abuse content if a notice has been issued but the content has not been taken down after a certain period of time?
14. Has online child sexual abuse content in your country decreased due to the work of your hotline?
15. What role do you think a notice and takedown scheme should play in a strategy designed to achieve the expeditious removal of internet child sexual abuse content?
16. What is the legal status of your hotline, e.g. national (local) organisation as a non-governmental organisation or member of an international organisation?
17. What is the preferred hotline model in your opinion in terms of its resource: government supported, ISP industry funded or independent?
18. If there is no hotline or it has been difficult to set up a hotline in your country relating to the removal of child sexual abuse content, what was the reason for that?
19. In your opinion, which one, blocking/filtering or an international notice and takedown, is more efficient in terms of the removal of child sexual abuse content? Any concern about the impact of blocking in your jurisdiction, e.g. privacy concern, freedom of expression, free access to information?
20. Are there any particular implementation issues you believe should be addressed in developing a comprehensive, transferable international notice and takedown best practice model relating to child sexual abuse content?

III. Relationship with stakeholders

21. What is the relationship between your hotline and ISPs?
22. Is there an agreement between your hotline and ISPs in terms of the removal of child sexual abuse content and other relevant issues, e.g. time frame for the notified content being taken down, data retention and sharing of a updated blocking list associated with child sexual abuse content?
23. What is the relationship between your hotline and local law enforcement agency?
24. Do you advise the Police before issuing notices to the ISPs? Do you wait for response from the Police and how long it is?

25. Has the work of your hotline been supported and encouraged by your local law enforcement agency such as the Police? What are the specific contributions your hotline has made from their point of view?
26. What is the relationship between your hotline and your government?

V. Documentation

Please attach to the completed questionnaire any other materials that can be used to supplement your views or would be beneficial to this research.

It will be greatly appreciated if you can send your response to weixiao@iwf.org.uk before Monday 31st May.

Thank you in advance for your co-operation and assistance with this research.

Please provide the following information for further communication

Name	
Position	
Organisation	
Country	
Address	
Telephone	
Email	