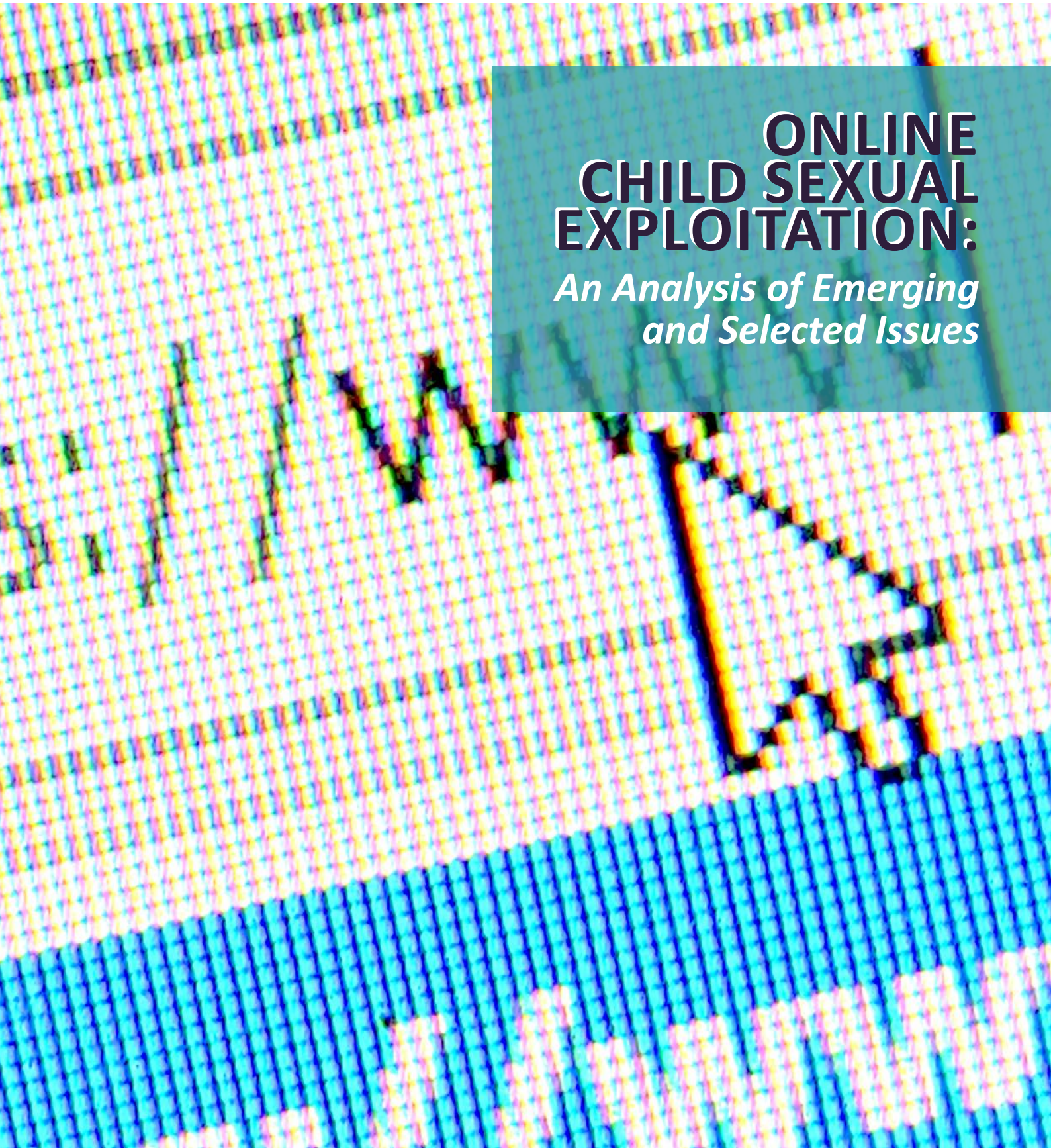
ECPAT International
JOURNAL
2017
ISSUE: 12 | APRIL, 2017



ONLINE CHILD SEXUAL EXPLOITATION:

An Analysis of Emerging and Selected Issues

ECPAT International

JOURNAL 2017

ISSUE: 12 | APRIL, 2017

Series Editor: Dr. Mark Capaldi

ECPAT International would like to thank John Carr, Madeleine van der Bruggen and David Parker for their review of the articles included in this Journal issue 12.

Layout & Design: Manida Naebklang

April, 2017

This publication was produced with the financial assistance of Irish Aid, Oak Foundation, Sida and Terre des Hommes Netherlands. The views expressed herein are solely those of the authors. The support received from the above-mentioned donors does not constitute endorsement of the opinions expressed.

Published by:

ECPAT International
328/1 Phaya Thai Road, Ratchathewi
Bangkok 10400 THAILAND
Tel: +662 215 3388, +662 611 0972
Fax: +662 215 8272
Email: info@ecpat.net
Website: www.ecpat.net

TABLE OF CONTENTS

PREFACE

Although information and communication technologies (ICTs) are an important and positive component of modern life, their rapid expansion is making more children vulnerable to online sexual exploitation. The swift evolution of the technology is leading to a terrifying growth in online child sexual abuse material (CSAM), as well as new emerging threats to children.

Without a doubt, the volume and scale of CSAM has reached unprecedented levels. In 2014, INHOPE, the association of INTERNET hotlines, assessed that 83,644 URLS containing child sexual abuse material exist worldwide, a 64% increase from the year before. The NCMEC Cybertipline (which handles reports of child sexual exploitation for major tech companies in the US) received more than 7.5 million reports since 1998, yet 4.4 million of these were received in 2015 alone. There is also a clear indication that child abuse material is being circulated by offenders through more hidden platforms, such as file sharing networks (including peer-to-peer), the 'Dark Net' or similarly encrypted software techniques such as The Onion Router (TOR).

ECPAT has a long record of contributing to global efforts aimed at eliminating online child sexual exploitation (OCSE). ECPAT advocates for the development and implementation of stronger, relevant legal frameworks; calls for the wider deployment of technical tools to reduce the availability of CSAM; supports law enforcement; and raises awareness with the public. ECPAT's Journal Series is yet another strategy to research, analyse and depict emerging global threats and trends in the sexual exploitation of children, including online, and to highlight lessons learnt and recommendations for better prevention and protection.

The latest ECPAT Journal predominately focuses on the online sexual exploitation of children. It contains four articles exploring some of the technical challenges and emerging concerns. The first article looks at how virtual currencies can be misused for child sex offending. It identifies that there are significant gaps in our knowledge of how the different virtual currencies can be used for illegal purposes, thereby raising the worrying issue of what exactly is the scale and scope of the problem? Fortunately, some opportunities for interventions are emerging.

Staying with technology, the second article looks at the effectiveness of filtering and blocking, in combination with the use of splash pages, as a mechanism to deny access to child sexual abuse material online. Despite promising results, the paper emphasises that the use of splash pages must still be used within a broader approach to tackling this problem, especially as some offenders will not be so easily deterred.

Not surprisingly, most of the efforts in tackling Internet child sex offending have focused on male perpetrators. However, an understudied aspect is the role played by women in the commission of ICT facilitated child sex offences. This article takes on the challenge of exposing female Internet sex offending and, in the process, presents some interesting findings on the specificity of female online sex offending. By understanding these nuances, more gender responsive interventions must be developed otherwise we will continue to miss this form of abuse and its child victims will remain hidden.

Finally, ECPAT concludes with another thought provoking article looking at the live streaming of child sexual abuse in the Philippines; one of the most significantly affected countries in the world. The article asks the question: 'why?'; especially when the country has a robust child protection legal framework. Clearly, domestic legal protection and regulatory frameworks alone are not sufficient to address this multi-faceted phenomenon as the Philippines is now realising.

This ECPAT Journal thus aims to highlight how the very nature of the Internet is resulting in the growth and evolution of online child sexual abuse materials. As such, ECPAT hopes that these articles can inform us of how the burgeoning online child sexual exploitation impacts everywhere and compels us to control its proliferation.

Dr. Mark Capaldi
Head of Research and Policy
ECPAT International

Virtual Currency Uses for Child Sex Offending Online

By: Yvonne Nouwen

INTRODUCTION

Financial services, such as banking, are increasingly offered through new and innovative methods, including those which use the Internet or mobile phone technology.[1] A new term has emerged to describe this burgeoning sector: *Fintech.* Additionally, a growing number of Internet-based payment services employ virtual currencies.

A virtual currency is a digital representation of value that is used and accepted among members of a specific community as a means of payment which can be transferred, stored or traded electronically.[2] There are different types of virtual currencies, but a characteristic of many is their ability to allow transactions without the entity at either end disclosing their real identity. These are known as 'crypto currencies' and Bitcoin is perhaps the best known example.

Because of this ability to facilitate anonymous transactions, crypto currencies are strongly associated with the sale of illegal items, or for funding other forms of criminality. Child sex offenders can employ crypto currencies when making payments related to their offending behaviour, thereby decreasing the risk of identification. This is especially the case when the use of virtual currencies is paired with additional anonymising tools and platforms meant for communicating and exchanging data.

This article explores virtual currencies and their potential misuse by child sex offenders online. First, the article elaborates on the distinction between virtual currencies and fiat,[3] or conventional currencies, and describes the different types of virtual currencies currently in use. The author also looks at the real and relative value to offenders of different kinds of virtual money as a potential means of exchange to be used for voluntary or extorted payments for child sexual abuse (material),[4] or for grooming[5] purposes. Additionally, elaborating on the pseudo anonymous nature of crypto currencies such as Bitcoin, this paper considers the limitations law enforcement and other agencies face in terms of identifying victims and investigating offenders.

A recurring issue in the article are the significant gaps in knowledge about the application of different types of virtual currencies for child sex offending online. Although evidence shows that specifically crypto currencies such as Bitcoin are

1 FATF/OECD (2014), "Virtual Currencies: Key Definitions and Potential AML/CFT Risks", FATF. Report, accessed 13 October 2016, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

2 European Banking Authority (2014), "EBA Opinion on virtual currencies", 5, accessed 8 September 2016, http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.

3 Fiat money is an intrinsically valueless object or record – i.e. printed paper – that is declared legal tender by government regulation or law and serves as a currency or medium of exchange. Examples are the U.S. Dollar and the Euro.

4 Child sexual abuse material - also referred to as child pornography- depicts acts of sexual abuse and/or focuses on the genitalia of the child. Child sexual exploitation material encompasses all other sexualised material depicting children. Information retrieved from Interagency Working Group (2016), "Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse" (hereinafter Luxembourg Guidelines), 40, accessed 27 October 2016, http://luxembourgguidelines.org/.

5 "In the context of child sexual exploitation and sexual abuse, "grooming" is the short name for the solicitation of children for sexual purposes. "Grooming/online grooming" refers to the process of establishing/building a relationship with a child either in person or through the use of the Internet or other digital technologies to facilitate either online or offline sexual contact with that person.", Luxembourg Guidelines, 51.

6 The International Monetary Fund (IMF) defines virtual currencies as "digital reresentations of value [...] which can be obtained, stored, accessed, and transacted electronically [...]" IMF (2016), "Virtual Currencies and Beyond: Initial Considerations", 7, accessed 19 September 2016, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf; The United States Government Accountability Office (GAO) refers to virtual currency as "a digital unit of exchange [...]", Richter, Kraus, et al. (2015), "Virtual Currencies like Bitcoin

employed for illegal purposes, many questions concerning the scope, scale and nature of their use in relation to child sex offending persist. The implication is a challenge in terms of the potential to develop adequate preventive or restrictive responses. This article provides an overview of the varying virtual currencies and links it to risks, future developments and opportunities for interventions against child sex offenders online.

VIRTUAL CURRENCIES: A DIGITAL REPRESENTATION OF VALUE

The term 'virtual currency' embraces two distinct ideas. 'Virtual' refers to something that is intangible, only in digital form and most commonly associated with the Internet. The common meaning of 'currency' is 'money', or something that is used as either a medium of exchange or a way of denoting value in financial terms. When literally translated, virtual currencies can therefore be explained as 'money which exists and is used or exchanged on the Internet.'

Virtual currencies need to be distinguished from 'simple' digital currencies such as electronic money (or e-money). While it is true that all virtual currencies are in essence digital,[6] it does not follow that all money exchanged digitally is virtual.

The European Union defines e-money as:

> *"A digital equivalent of cash, stored on an electronic device or remotely at a server. One common type of e-money is the 'electronic purse', where users store relatively small amounts of money on their payment card or other smart card, to use for making small payments. But e-money can also be stored on (and used via) mobile phones or in a payment account on the Internet."*[7]

Thus, e-money will normally always be expressed first in terms of an existing real world, fiat currency, but is transferred or stored online.

By contrast in 2014 the European Banking Authority defined a virtual currency as:

> *"A digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons*[8] *as a means of payment and can be transferred, stored or traded electronically."*[9]

In other words, the difference with virtual currencies is that e-money's reference is always to a fiat currency or money with legal tender status,[10] whereas a virtual currency is expressed in its own terms.

as a Paradigm Shift in the Field of Transactions", International Business & Economics Research Journal Volume 14, no. 4 (2015): 578); Similarly the Financial Action Task Force (FATF) defines virtual currencies as "a digital representation of value that can be traded on the Internet [..]", FATF/OECD (2014), 'Virtual Currencies: Key Definitions and Potential AML/CFT Risks', FATF Report, 4, accessed 8 September 2016, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf. These digital representations have their own digital unit of account, such as Bitcoins, Linden Dollars and E-Gold.

7 European Commission (2016), "Banking and Finance: E-Money", accessed 24 January 2017, http://ec.europa.eu/finance/payments/emoney/index_en.htm.

8 A natural person in legal meaning is an individual human being as opposed to a legal person which may be a private or public organisation (for example a business company or non-governmental organisation).

9 European Banking Authority (2014), "EBA opinion on virtual currencies", 11, accessed 24 January 2017, https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.

10 World Bank (2012), "Innovation in retail payments worldwide: a snapshot", 10-17, July 2012.

The fact that virtual currencies digitally represent a value or currency does not imply that they do not have a 'real-world value'. In fact, depending on the underlying payment mechanism, virtual currencies can be exchanged with fiat currencies and be used for payments for goods and services in the real economy.[11] Convertible virtual currencies can be bought and/or sold for fiat money and can be used to buy virtual and/or real goods and services (e.g. Bitcoins).[12] However, non-convertible or closed virtual currencies cannot be exchanged or bought for fiat currency and have almost no link to the 'real' world but rather are specific to a virtual world (e.g. gaming money).[13]

Virtual currencies are also categorised according to their operated, with on one hand, the centralised virtual currencies that - much like 'traditional' fiat money - have a single administrating authority which issues the currency, establishes and implements the rules for its use and circulation and maintains a central payment ledger. Decentralised virtual currencies, on the other hand, have neither a central administrating authority nor central oversight; rather authority is decentralised among the participants or users of the currency.[14]

Decentralised virtual currencies rely on cryptography, or the application of mathematical calculations by specific members (so called 'miners') of the peer-to-peer network to ensure that the total balance of the ledger is and remains correct.[15] This means authority is decentralised among the participants or users of the currency.[16] Because of the application of cryptography, these currencies are referred to as 'cryptocurrencies', with Bitcoin[17] being the most familiar.

ANONIMITY: THE APPEAL OF VIRTUAL CURRENCIES – PARTICULARLY BITCOINS – FOR CHILD SEX OFFENDING

Bitcoins and other crypto currencies are often associated with anonymity since they withhold identifying information that can be reliably reproduced should it be necessary to locate or identify the users of the currency. Because of this (pseudo) anonymous nature, they are repeatedly linked to secret or illegitimate transactions.

11 IMF (2016), "Virtual Currencies and Beyond: Initial Considerations", 7, accessed 19 September 2016, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf.

12 One-way flow convertible virtual currencies can be bought or awarded against a specific conversion rate but cannot be exchanged back into fiat money. This type of currency is akin to a coupon and can be used to buy virtual goods and services and with exception also to buy real goods and services (European Central Bank (2012), "Virtual Currency Schemes", 5, accessed 27 October 2016, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf). An example is online music vouchers such as the I-tunes gift cards which can be bought online, send to a recipient per e-mail and can be used to purchase and download songs and (music) albums.

13 Bidirectional flow convertible currencies are comparable with any other real currency and can be bought and sold with fiat money and converted back to 'real' currencies. This type of convertible virtual currency can be used for making purchases online and offline. European Central Bank (2012), "Virtual Currency Schemes", 5, accessed 27 October 2016, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

14 The value of non-convertible or closed virtual currencies stems from the governing rules of the corresponding virtual community which assures the currency. An example is virtual money used in Massively Multi-Player Online Role-Playing Games (MMORPGs) such as 'World of Warcraft'. These game currencies usually can only be earned by online performance and no exchanges or purchases outside the specific virtual community are (officially) possible. Rather, this virtual currency is to be spent within the virtual (gaming) platform it serves, for example to purchase virtual weapons, avatars or real estate. Richter, Kraus, et al. (2015), "Virtual Currencies like Bitcoin as a Paradigm Shift in the Field of Transactions".

15 Yamaguchi, Hiroshi (2004), 'An Analysis of Virtual Currencies in Online Games', Tokyo: Komazawa University.

16 Richter, Kraus, et al. (2015), "Virtual Currencies like Bitcoin as a Paradigm Shift in the Field of Transactions".

17 Decentralised virtual currencies offer a publicly available online distributed transaction ledger – also referred to as 'the block chain' - which can only be changed if the block chain participants (i.e. users of the virtual currency) agree with a transaction. Each transaction has to be verified by the 'miners' or those users who apply cryptography to check and verify transactions, before it is recorded on the "block" and added to the end of the 'chain', thereby changing the overall balance. If anyone tries to tamper with one ledger, all of the 'nodes' (block chain participants) will disagree on the integrity of that ledger and will refuse to incorporate the transaction into the block chain, thereby blocking the transaction. The entire block-chain or transaction history is available as well as searchable for all the currency community members. Paar, Christof and Jan Pelzl, (2010),"Understanding Cryptography: A Textbook for Students and Practitioners", Chapter 6: 149 – 172, Berlin: Springer-Verlag.

In fact, various parties including the FBI[18] and Europol[19] warn about the risks of virtual currencies, particularly crypto currencies, being an attractive payment system for those trying to trade illicit goods, including child sexual abuse materials.

However, the characteristics of Bitcoin and similar crypto currencies do not necessarily make them equipped to provide anonymity. In fact, currencies using a decentralised public ledger system or the block-chain technology do not hide transactions.[20] Rather, they ensure a high level of transparency, providing permanent access to Bitcoin community members to search and view transaction histories in their entirety. Every user can see the balance and all transactions of any Bitcoin address at any time.[21]

The anonymity stems from the fact that Bitcoin users do not have to disclose who they are. Instead, Bitcoin users are only represented within the system through their Bitcoin address. These Bitcoin addresses consist of a string of letters and numbers not systematically linked to an individual, therefore providing a level of anonymity.[22] This anonymity however, is at stake when users employ their virtual currency to purchase goods or services from parties who require them to reveal their identity; for example, by providing address details to receive a package. Once the user discloses identifying information, all of the other publicly visible, but previously anonymous, purchases conducted with the same Bitcoin address can be traced back to that information.[23]

Unsurprisingly then, the transparency of the block chain technology used in Bitcoin is a primary concern for criminal users.[24] To maintain anonymity, users can generate and use a new Bitcoin address (i.e. encryption key) for each transaction to prevent purchases from being linked to the same user. Generally, each user has hundreds of different Bitcoin addresses that are all stored and transparently managed by a digital wallet.[25] Additionally, as long as users refrain from using their virtual currencies for exchanges with third parties requesting or representing identifying information, they can remain anonymous. However, to some extent the users are also dependent on how careful those they are exchanging currencies with are, in terms of avoiding identification and giving away information about their transactions.

So considering all of those limitations, how appealing is Bitcoin for child sex offenders as a payment method? For child sex offenders the anonymity or pseudo-anonymity ensured by crypto currencies provides them with an opportunity to make transactions online for something with which they do not want to be associated. And although when it comes to the exchange of child sexual abuse material, most of the material is still largely distributed and available non-commercially - in fact, new material can actually function as a currency in itself - commercial distribution also occurs.[26]

Data from INHOPE indicates that 9% of child sexual abuse material which was shared online in 2014 was commercial in nature; meaning that

18 Bitcoin is the world's first completely decentralised digital payment system (Brito, Jerry and Andrea Castillo (2013), "Bitcoin: a Primer for Policymakers", Arlington: Mercatus Center.

19 FBI (2012), "Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity", USA: Federal Bureau of Investigations.

20 Europol (2013), "Work Package 2: Strategic Assessment of Commercial Sexual Exploitation of Children Online", 12, accessed 11 October 2016, http://www.safenet.bg/images/sampledata/files/efc_strategic_assessment_-_public_version.pdf.

21 Brito, Jerry and Castillo, Andrea (2013), "Bitcoin: a Primer for Policymakers", Arlington: Mercatus Center.

22 Bitcoin (2016), "Protect your Privacy", accessed 22 September 2016, https://bitcoin.org/en/protect-your-privacy.

23 FATF/OECD (2014), "Virtual Currencies: Key Definitions and Potential AML/CFT Risks", FATF Report, 6, accessed 13 October 2016, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

24 Bitcoin (2016), "Protect your Privacy", accessed 22 September 2016, https://bitcoin.org/en/protect-your-privacy.

25 Europol (2016), "Internet Organised Crime Threat Assessment 2016", 42, accessed 7 September 2016, http://docplayer.net/22881872-Iocta-2016-internet-organised-crime-threat-assessment.html#show_full_text.

26 Androulaki, Elli, et al. (2012), "Evaluating User Privacy in Bitcoin", 35, accessed 7 September 2016, https://eprint.iacr.org/2012/596.pdf.

a financial transaction is required to access the content.[27] Law enforcement cases in the past also demonstrate that it can be quite profitable to engage in the selling of child sexual abuse material.[28] There are instances of child sexual abuse material being exchanged via anonymous platforms in return for Bitcoins.[29] Additionally, other anonymous or difficult-to-trace electronic payments forms emerged in relation to payments for child sexual abuse materials.[30]

By using decentralised cryptocurrencies such as Bitcoin, child sex offenders can ensure that both buyer and seller avoid identification as much as possible by maintaining a certain level of anonymity. There is an apparent migration of online child sexual exploitation from more traditional payment systems (such as credit cards) to anonymising tools and (pseudo) anonymous payment systems including virtual currencies.[31] This can be attributed to the wide availability of more anonymous payment methods, as well as the proactive measures put in place by payment system providers such as PayPal and Western Union to prevent the use of their service for illegal purposes.

In order to anonymously proceed with their criminal acts, offenders not only need to know how to use such currencies securely; they also need to be able to use other encryption tools and anonymous platforms to ensure all of their acts evade detection. Crypto currencies typically do not provide a means to communicate anonymously among the users, or exchange other data or resources other than the virtual currencies. This implies that for the purpose of clarifying or agreeing on, among other things, the amount, nature and the date of transactions, or for their communication with (potential) victims, offenders must deploy various other encryption tools to evade detection. Many offenders use peer-to-peer (P2P) networks[32] to communicate and exchange child sexual abuse material with other perpetrators, including encrypted services such as TOR.[33] In addition, offenders use encrypted cloud services[34] to store and share data.

For their communication with children and potential victims, offenders use a variety of different platforms. Often online contact is initiated through social media sites, gaming

27 INHOPE (2014), "Statistics and Infographics: Worldwide commercial hosting in 2014", accessed 9 October 2016, http://www.inhope.org/Libraries/Statistics_Infographics_2014/INHOPE_stats_infographics_for_2014.sflb.ashx.

28 For example, in 2001 the FBI investigated a website operated by 'Landslide Productions', whereby the perpetrators were selling subscriptions to websites offering child sexual abuse material, grossing $1.4 million dollars in one month which demonstrates the potential profit involved in exchanging or making available child sexual abuse material. Information retrieved from Taylor, Max, et al. (2003), "Child Pornography: An Internet Crime", accessed 10 October 2016, https://www.researchgate.net/publication/229646969_Child_Pornography_An_Internet_Crime.

29 Europol (2014), "The Internet Organised Crime Threat Assessment 2014: Chapter 3.3 Child sexual exploitation online Overview", accessed 21 September 2016, https://www.europol.europa.eu/iocta/2014/chap-3-3-view1.html.

30 European Banking Authority (2014), "EBA Opinion on virtual currencies", 10, accessed 8 September 2016, http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.

31 *Ibid*., Key Threat - Commercial distribution.

32 Following the NetClean Report 2016, peer-to-peer networks are the most common way to share material and it is also where the majority of the material is shared according to 90% of the police officers interviewed. NetClean (2016), "The NetClean report 2016", accessed 22 December 2016, http://www.netclean.com/wp-content/uploads/2016/12/NetClean_Report_2016_English_print.pdf. A peer-to-peer (P2P) network simplifies media exchange among users by offering them the possibility to directly connect to each other via largely ad hoc connections and the cumulative bandwidth of network participants. Users of the decentralised network are allowed to be the direct provider of content to the other users on the network and also the direct consumer of content without a central server in-between. Such networks are used amongst other things to share content files containing audio, video data or anything in digital format. Information retrieved from Johnsson, Andreas and Avodele Damola (2008), "Peer to Peer Network", accessed 28 October 2016, https://docs.google.com/viewer?url=patentimages.storage.googleapis.com/pdfs/US20110270924.pdf.

33 43% of police officers interviewed for the Netclean Report 2016 indicated TOR and the Darknet (anonymous websites and encrypted networks that are most commonly reached via TOR) are the methods most commonly used to share and distribute child sexual abuse material. NetClean (2016), "The NetClean report 2016", accessed 22 December 2016, http://www.netclean.com/wp-content/uploads/2016/12/NetClean_Report_2016_English_print.pdf. TOR Software is used to conceal user's identities and their online activity from surveillance and traffic analysis by redirecting online traffic (for example an e-mail) through a dynamically assigned route using an encrypted connection. This way it is not clear where data is coming from or where it is going, providing a level of anonymity for the sender and receiver. Information retrieved from ECPAT International (2015), "Internet and Technology Factsheet: what is TOR?", accessed 6 September 2016, http://www.ecpat.org/resources/.

platforms and other virtual spaces where a lot of children are present, but which are not necessarily anonymous in nature.

For the purpose of sharing photos and (live) videos, offenders can suggest they migrate to more anonymous platforms where they proceed with acts of grooming or sexual extortion. As part of the online grooming process, offenders can make payments to children to gain their trust and/or convince them to share material of a sexual nature of themselves. Or, as part of financially driven (sexual) extortion, after obtaining compromising photos or videos of a sexual nature, offenders can pressure the victim into paying amounts of money by threatening to disclose the images on the Internet or saying they will send it to the child's peers or relatives if he/she does not pay. These payments can be conducted with both real currencies, as well as virtual currencies.

Closed virtual currencies, as explained before, might have less value for those offenders or facilitators who are financially driven as they can only be used within very specific online communities to purchase virtual goods or services. However, this type of virtual money could serve as a currency of exchange in processes of grooming and sexual extortion of children.

Particularly, this the case in Massive Multi-user Online Role-Playing Games (MMORPGs). Offenders are already using voice and text chat functions in online gaming platforms to groom children.[35] MMORPGs generally have their own virtual closed currency or 'gaming money', which is difficult to acquire yet essential in order to progress in the game.

Players in a gaming community often build strong virtual relationships; in fact, social interaction is often paramount in order to advance within the game.[36] Offenders can build on those interdependent relationships to sexualise the interaction progressively.[37] It is not difficult to imagine that virtual gaming currencies or commodities, just like (promises of) fiat money or gifts, can be used as part of grooming processes to gain the child's trust, meet the 'needs' of the child (i.e. wanting to progress in the game) and eventually manipulate them to engage in sexual activities. Although there is not much literature or evidence yet as to what extent virtual (closed) currencies are used as part of these grooming behaviours, it is likely that this could be part of child sex offenders' modus operandi.

CAUSE FOR ALARM: LIMITED OPPORTUNITIES TO OBSTRUCT OFFENDERS

The significance of child sex offenders using virtual (crypto) currencies is the difficulty in identifying who they are, especially when the use is paired with the use of other anonymising tools and platforms.[38] The increased application of such tools represents an additional obstacle and signifies that it is getting more and more complicated for law enforcement authorities

34 In the Netclean Report 2016 it is indicated that police officers witness an increasing trend of child sexual abuse material being distributed through cloud based services. NetClean (2016), "The NetClean report 2016", accessed 22 December 2016, http://www.netclean.com/wp-content/uploads/2016/12/NetClean_Report_2016_English_print.pdf). Cloud Computing involves services which are instantly available for users (on demand) and are provided for free or on a pay-per-use basis. Rather than running programmes or storing data on their own hardware (e.g. computer, hard drive), users use remote servers for which the necessary infrastructure and applications are hosted by the cloud service companies. Ever more services and personal data are moving into the cloud such as e-mail, pictures, banking services and storage space. Information retrieved from ECPAT International (2015), "Internet and Technology Factsheets: What is Cloud Computing?", accessed 28 October 2016, http://www.ecpat.org/resources/.

35 Katersky, Aaron (2012), "Online gaming is becoming predator's playground", accessed 16 September 2016, http://abcnews.go.com/US/online-gaming-predators-playground/story?id=16081873.

36 Task Force on the Digital Economy (2014), "The Digital Economy: Potential, Perils and Promises", accessed on 7 November 2016, http://innovation.luskin.ucla.edu/sites/default/files/DETF_report.pdf.

37 Young, Kimberly (2009), "Understanding Online Gaming Addiction and Treatment Issues for Adolescents", *The American Journal of Family Therapy, 37* (2009): 355 – 372.

38 European Banking Authority (2014), "EBA Opinion on virtual currencies", 10, accessed 8 September 2016, http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.

to apprehend offenders and bring an end to the sexual abuse and exploitation through identification, investigation and prosecution. Chances of apprehension mainly depend on mishaps by the offenders themselves or by those they are communicating with. Often, offenders are only caught when they make mistakes.[39]

Additionally, there are other limitations crypto currencies pose in relation to opportunities for identification and apprehension of online child sex offenders. Since decentralised virtual currencies, including crypto currencies, do not have a central administering authority nor are centrally monitored, there is not one point of contact or entity which can be held accountable for their services being used for illegal purposes. In fact, up until today it is unknown who created Bitcoin and it is widely believed that the name linked to the crypto currency 'Satoshi Nakamoto' is just a pseudonym for the person or persons who created Bitcoin.[40]

Not having a central point of contact or central authoritative body implies that law enforcement cannot approach someone with a request for additional information for the sake of an investigation if needed. Authorities can however, target individual exchangers for client information that the exchanger may collect, but there is no central database or point of information.[41]

Nor is there a central intermediary that could be required to notify authorities of suspicious transactions for illegal purposes, including the commercial exchange of child sexual abuse material. Additionally, the lack of a central issuing entity that administrates the total balance undermines the possibility to impose financial sanctions and seizure of assets as it is very difficult, if not impossible, to impose financial sanctions and embargoes on an entire network of peers.[42] Sudden changes in the (distributed) ledger will not be accepted by the system unless the network of nodes or users agrees to the alteration, again restricting options for law enforcement authorities to intervene.

Finally, virtual currencies are used and accepted worldwide and across jurisdictional boundaries. They often rely on complex infrastructures involving segmented service provision, with different entities across borders responsible for collecting customer/transaction records and conducting transactions. These transactions are by their nature, irreversible. All of these factors hamper access and intervention options for law enforcement and regulators.[43]

Despite all of these factors, Bitcoin and similar decentralised virtual (crypto) currencies are considered to not provide true anonymity or 'security' for their users. Various experiments and investigations have demonstrated that there may be ways to identify users of Bitcoin by looking at the patterns of their transactions.[44] Therefore, users and developers are seeking to enhance the anonymity of virtual currencies.

There are and have been new virtual (crypto) currencies in development that seek to provide additional layers of anonymity and redress the issue of transparency as provided by currencies using a transparent block-chain system, such as Bitcoin. So called 'mixing services' and new crypto currencies (e.g. Anoncoin, Darkcoin and most recently Zcash blockchain[45]) have come up which ensure that even a user's pseudonymous identity can remain private.[46] Although this 'complete' anonymity may be useful for legitimate purposes, such as protecting

39 Task Force on the Digital Economy (2014), "The Digital Economy: Potential, Perils and Promises", 12-13, accessed 7 November 2016, http://innovation.luskin.ucla.edu/sites/default/files/DETF_report.pdf.

40 Lustig, Caitlin and Nardi, Bonnie (2015), "Algorithmic Authority: The Case of Bitcoin", accessed 7 November 2016, http://www.artifex.org/~bonnie/lustig_nardi_HICSS_2015.pdf

41 FATF/OECD (2014), "Virtual Currencies: Key Definitions and Potential AML/CFT Risks", FATF Report, 15, accessed 15 October 2016, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

42 European Banking Authority (2014), "EBA Opinion on virtual currencies", accessed 8 September 2016, http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.

43 FATF/OECD (2014), "Virtual Currencies: Key Definitions and Potential AML/CFT Risks", FATF Report, 15.

44 For example, in 2013, staff at the University of California found that even though the Bitcoin protocols do not allow for connecting a transaction directly to a specific person, through examining patterns of transactions, users may be identified. Information retrieved from Task Force on the Digital Economy (2014), "The Digital Economy: Potential, Perils and Promises", 13, accessed 7 November 2016, http://innovation.luskin.ucla.edu/sites/default/files/DETF_report.pdf.

journalists and dissidents from oppressive governments, it is not difficult to imagine that an inevitable outcome of this anonymity may be its appeal to those trying to engage in illegal conduct.

According to Europol, a continued increase in the use of payment systems that offer more anonymity than traditional payment methods is to be expected and they may become the currency of choice for various manifestations of child sexual exploitation online, including financially driven sexual extortion of children and live online child sexual abuse.[47]

CONCLUSION: STATE OF AFFAIRS AND RECOMMENDATIONS FOR THE FUTURE

Virtual currencies provide a payment method that could change the state's control over money and make way for more transparent payment systems. At the same time, they offer a reduction in transaction costs.[48] In addition, virtual (crypto) currencies using block-chain technology, can provide a level of transparency that historically has not been seen in traditional currencies and their exchange. These newer approaches allow any user at any time to see all the transactions that have ever been made, yet at the same time provide a level of anonymity or privacy which many users find important in the increasingly connected online world, where data lives on forever.

Many of these positive factors, as well as perfectly legitimate uses, are still pertinent today and virtual currencies came into existence for entirely understandable reasons.[49] Therefore, there is no suggestion crypto currencies should be outlawed or their use to be declared to be beyond the pale. However, it is important to understand that anonymity is a double-edged sword as it can facilitate and potentially encourage child sex offenders in commencing or continuing their activities online with little risk of apprehension. With that in mind, it is vital that we see what measures can be taken that recognise the core features of virtual and crypto currencies but can help to prevent its illegal use by people such as child sex offenders.

New anonymous payment services are on the horizon. They appear to be able to offer even higher levels of anonymity than those currently available. This issue is not going away. Nor is it likely to reduce in importance. It is therefore vital to enhance our understanding of crypto currencies and how they are being used by child sex offenders. Although there is evidence showing *why* virtual currencies are attractive to child sex offenders, little is known about the *broader scope*, *scale* and *nature* of their uses. Such knowledge is necessary for understanding the extent to which they actually do facilitate or promote child sex offending and to help develop strategies to prevent or intervene to interdict it.

Considering their expertise and experience in developing, implementing, monitoring and/or using virtual currencies, it is paramount to cooperate with the virtual currency (developers) sector to increase our understanding of its use and the opportunities to intervene, if necessary. In addition, it could be worthwhile to look at how more traditional payment methods are regulated and which self-regulatory mechanisms and formal commitments promoting responsible business practices (for example know-your-customer principles and transaction monitoring obligations) are in place to prevent currencies from being used for illegitimate purposes. It would help to explore to what extent and how – if, at all - such lessons could be interpreted and applied to virtual currencies, in particular crypto currencies. Finally, it is necessary to seek cooperation with and increase our understanding of some of the sub cultures which are developing in the virtual currency space, particularly around the gaming industries such as MMORPGs.

45 Hackett, Robert (2016), "Meet the latest hyped Cryptocurrency", accessed 8 November 2016, http://fortune.com/2016/10/29/zcash-bitcoin-cryptocurrency/.

46 Bonneau, Joseph, et al. (2014), "Mixcoin : Anonimity for Bitcoin with Accountable Mixes", 1-2, Princeton University: Princeton, USA.

47 Europol (2016), "Internet Organised Crime Threat Assessment 2016", 27, accessed 7 September 2016, http://docplayer.net/22881872-Iocta-2016-internet-organised-crime-threat-assessment.html#show_full_text.

48 *Ibid*., 1-2.

49 Richter, Kraus, *et al*. (2015), "Virtual Currencies Like Bitcoin As A Paradigm Shift In The Field Of Transactions".

BIBLIOGRAPHY

Androulaki, Elli, et al. (2012), "Evaluating User Privacy in Bitcoin", 35, accessed 7 September 2016, https://eprint.iacr.org/2012/596.pdf

Bitcoin (2016), "Protect your Privacy", accessed 22 September 2016, https://bitcoin.org/en/protect-your-privacy

Bonneau, Joseph, *et al.* (2014), "Mixcoin : Anonimity for Bitcoin with Accountable Mixes", Princeton University: Princeton, USA.

Brito, Jerry and Andrea Castillo (2013), "Bitcoin: a Primer for Policymakers", Arlington: Mercatus Center.

ECPAT International (2015), "Internet and Technology Factsheets: What is Cloud Computing?", accessed 28 October 2016, http://www.ecpat.org/resources/.

ECPAT International (2015), "Internet and Technology Factsheet: what is TOR?", accessed 6 September 2016, http://www.ecpat.org/resources/.

European Banking Authority (2014), "EBA Opinion on virtual currencies", accessed 8 September 2016, http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.

European Central Bank (2012), "Virtual Currency Schemes", accessed 27 October 2016, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

European Commission (2016), "Banking and Finance: E-Money", accessed 24 January 2017, http://ec.europa.eu/finance/payments/emoney/index_en.htm.

European Financial Coalition (2015), "Commercial Sexual Exploitation of Children Online : A Strategic Assessment", accessed 6 September 2016, http://www.europeanfinancialcoalition.eu/private10/images/document/21.pdf.

Europol (2013), "Work Package 2: Strategic Assessment of Commercial Sexual Exploitation of Children Online", accessed on 11 October 2016, http://www.safenet.bg/images/sampledata/files/efc_strategic_assessment_-_public_version.pdf.

Europol (2014), "The Internet Organised Crime Threat Assessment 2014: Chapter 3.3 Child sexual exploitation online Overview", accessed 21 September 2016, https://www.europol.europa.eu/iocta/2014/chap-3-3-view1.html.

Europol (2016), "Internet Organised Crime Threat Assessment 2016", accessed 7 September 2016, http://docplayer.net/22881872-Iocta-2016-internet-organised-crime-threat-assessment.html#show_full_text.

FATF/OECD (2014), "Virtual Currencies: Key Definitions and Potential AML/CFT Risks", FATF Report 2014, accessed 13 October 2016, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

FBI (2012), "Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity", USA: Federal Bureau of Investigations.

Hackett, Robert (2016), "Meet the latest hyped Cryptocurrency", accessed 8 November 2016, http://fortune.com/2016/10/29/zcash-bitcoin-cryptocurrency/.

IMF (2016), "Virtual Currencies and Beyond: Initial Considerations", accessed 19 September 2016, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf.

INHOPE (2014), "Statistics and Infographics: Worldwide commercial hosting in 2014", accessed 9 October 2016, http://www.inhope.org/Libraries/Statistics_Infographics_2014/INHOPE_stats_infographics_for_2014.sflb.ashx.

Interagency Working Group (2016), "Terminology and Semantics", accessed 27 October 2016, http://luxembourgguidelines.org/.

Johnsson, Andreas and Avodele Damola (2008), "Peer to Peer Network", accessed 28 October 2016, https://docs.google.com/viewer?url=patentimages.storage.googleapis.com/pdfs/US20110270924.pdf.

Katersky, Aaron (2012), "Online gaming is becoming predator's playground", accessed 16 September 2016, http://abcnews.go.com/US/online-gaming-predators-playground/story?id=16081873.

Lustig, Caitlin and Nardi, Bonnie (2015), "Algorithmic Authority: The Case of Bitcoin", accessed 7 November 2016, http://www.artifex.org/~bonnie/lustig_nardi_HICSS_2015.pdf.

NetClean (2016), "The NetClean report 2016", accessed 22 December 2016, http://www.netclean.com/wp-content/uploads/2016/12/NetClean_Report_2016_English_print.pdf.

Paar, Christof and Pelzl, Jan, (2010), "Understanding Cryptography: A Textbook for Students and Practitioners", Chapter 6: 149 – 172, Berlin: Springer-Verlag.

Richter, Kraus, *et al.* (2015), "Virtual Currencies like Bitcoin as a Paradigm Shift in the Field of Transactions", *International Business & Economics Research Journal* Volume 14, no. 4 (2015): 575-586.

Task Force on the Digital Economy (2014), "The Digital Economy: Potential, Perils and Promises", accessed 7 November 2016, http://innovation.luskin.ucla.edu/sites/default/files/DETF_report.pdf.

Taylor, Max, et al. (2003), "Child Pornography: An Internet Crime", accessed 10 October 2016, https://www.researchgate.net/publication/229646969_Child_Pornography_An_Internet_Crime.

World Bank (2012), "Innovation in retail payments worldwide: a snapshot", 10-17, July 2012.

Yamaguchi, Hiroshi (2004), 'An Analysis of Virtual Currencies in Online Games', Tokyo: Komazawa University.

Young, Kimberly (2009), "Understanding Online Gaming Addiction and Treatment Issues for Adolescents", *The American Journal of Family Therapy,* 37 (2009): 355 – 372.

The Effectiveness of Splash Pages as a Deterrece Measure

By: Yvonne Nouwen

INTRODUCTION

As online technologies evolve, so do the methods used by offenders to acquire, distribute and search for child sexual abuse material (CSAM). The search for such content can be obstructed primarily in two ways: reducing its availability online, and restricting access. Usually, access to child sexual abuse images is restricted by means of filtering and blocking procedures which deny users entry to online locations that are known to contain child sexual abuse content. These filtering and blocking mechanisms may be complemented with splash pages which provide deterrence messages for example, warning users about the illegality of the searched for content and their actions, offering means to access help for those struggling with deviant sexual interests and/or linking to mechanisms to report child sexual abuse content online.

Research demonstrates that deterrence measures can be effective in obstructing and denying access to CSAM.[1] However, it is not clear to what extent the use of splash pages, as an added measure to filtering and blocking procedures, contributes to the reduction of child sexual abuse material searches.

This article explores the extent and ways in which splash pages contribute to deterring offenders from accessing and sharing child sexual abuse material online. It looks at the different methods used to filter and block child sexual abuse material as a prerequisite for splash pages targeting users who try to access such content. The ways in which deterrence messages can affect Internet users landing on a splash page are also discussed to consider its added value in an approach to combating child sexual abuse content online.

SPLASH PAGES AS A FINAL STEP IN A FILTERING AND BLOCKING SCHEME

A splash page refers to an introductory page preceding the homepage of an organisation or business. Rather than stating the purpose and nature of the website to be accessed, a splash page usually contains visual material and indirect expressions about the organisation or company's mission and provides advertising information.[2] A splash page may 'pop up' in the user's screen unexpectedly after or before visiting a certain page or online content.[3] Depending on how the webmaster programmed the splash page, the user can skip the splash page by clicking a 'skip intro' button, or similar message. In some cases however, this feature is not included, making it impossible to ignore the page.[4]

Splash pages are used for different reasons. Some aim to draw users in, others to keep them out.[5] They may attract the visitor's attention to

1 For example, the deployment of technical controls by Microsoft and Google – including enhanced filtering and blocking of child sexual abuse material-related queries as well as deterrence messaging – has had a rapid and significant impact on child sexual abuse material searches. Research showed a precipitous drop in such searches of 67% after Microsoft and Google announced their measures to the world. Information retrieved from Steel, C.M.S. (2015) "Web-based child pornography: The global impact of deterrence efforts and its consumption on mobile platforms", Child Abuse & Neglect, 2015.5.

2 Kim, H., Coyle, J.R. and Gould, S.J. (2009), "Collectivist and Individualist Influences on Website Design in South Korea and the U.S.: A Cross-Cultural Content Analysis," *Journal of Computer-Mediated Communication*: 14 (2009), 581-601.

3 *Ibid.*

4 KG Blog, (n.d.), "Flash pages"; accessed 6 March 2015. https://www.karelgeenen.nl/termen/splash-page/.

5 Kim, "Collectivist and Individualist influences".

6 Lennartz, Sven (n.d.), "Splash pages: do we really need them?" Smashing Magazine; accessed 9 March 2015. http://www.smashingmagazine.com/2007/10/11/splash-pages-do-we-really-need-them/.

7 UN Human Rights Council (2014), "Report of the Special Rapporteur on the sale of children, child prostitution and child pornography, Maud de Boer-Buquicchio", UN Doc. A/HRC/28/56, 22 dECEMBER 2014, para. 67-68.

an important message or display disclaimers or warnings that are supposed to restrict access.[6] This also accounts for splash pages which aim to limit access to CSAM. To understand the use of splash pages for the purpose of deterrence, it is first important to consider how this tool fits into the broader framework of measures deterring child sex offenders online.

Splash pages can be considered as more or less, the final product or output in a deterrence scheme involving filtering and blocking. Filtering and blocking technologies are an example of the opportunities for preventing access to online child sexual abuse content.[7] The increased diversity of information available on online systems and networks is leading governments, corporations, individuals, groups and Internet Service Providers (ISPs) to implement policies and more controls to either filter or otherwise limit the availability of inappropriate or undesirable content for end users.

Content access control policies typically block undesirable content from reaching all, or a subset of, end users in a given online service and/or network.[8] Content is often blocked for being offensive or inappropriate for a user group, or for viewing at a particular time of day or other similar reasons. For example, some governments apply nationwide systems to restrict their citizen's access to content, such as news, politics and entertainment.[9] Companies, schools and public libraries sometimes apply filters to block adult content as well as access to social networking sites, games and entertainment during office/school hours in order to improve productivity and prevent users from accessing harmful content. Some systems allow end users to select their own self-imposed set of blocking policies.[10] For example, parental control options or applications can be used to block content which is deemed age-inappropriate for children of different age groups.[11]

There are many different reasons why filtering and blocking is applied and supported by different users, but filtering and blocking is not without its' critics. An issue raised by every filtering regime is the extent to which blocking is either too broad, restricting access to content which should be accessible following the norms and/or rules of the applied filtering scheme (also referred to as 'over-blocking'), or not broad enough thereby missing undesirable or illegal content in filtering and blocking efforts (also referred to as 'under-blocking').

This is due to the fact that filtering and blocking are usually applied in an automated manner to a vast and dynamic system, the Internet, thereby losing the ability to apply a nuanced approach or assess either the context or the content's meaning before categorising and filtering it as being desirable or undesirable. Over-blocking in particular, receives much criticism for affecting human rights, specifically from those advocating for freedom of expression, freedom to information, privacy, religion and association.[12]

With regard to CSAM – as far as there is consensus about what it constitutes – there seems to be general support for filtering and blocking of such content. Internet Service Providers can block child sexual abuse material for the user population as a whole at any time on their own initiative, or in response to orders by courts or administrative authorities issuing them to remove or disable access to illegal content. Some legal acts and directives obligate Internet Service Providers and States to take measures to remove or disable access to child sexual abuse content which is hosted on their service upon obtaining such knowledge or awareness.[13]

---

8 Massarani, Leonardo C. (2002), "Content-indexing search system and method providing search results consistent with content filtering and blocking policies implemented in a blocking engine", *International Business Machines Corporation,* accessed 10 March 2015, https://docs.google.com/viewer?url=patentimages.storage.googleapis.com/pdfs/US6336117.pdf.

9 Palfrey Jr., John G. (2011), "Local Nets on aGlobal Network: Filtering and the Internet Governance Problem", in *The Global Flow of Information: Legal, social and cultural perspectives*, eds. Subramanian, Ramesh and Eddan Katz, New York: NYU Press.

10 Massarani, Leonardo C. (2002), "Content-indexing search system and method providing search results consistent with content filtering and blocking policies implemented in a blocking engine".

11 Heins, Marjorie and Cho, Christina (2001), "Internet Filters: A Public Policy Report", *Free Expression Policy Project*, accessed on 9 November 2015, http://ncac.org/wp-content/uploads/import/Internet%20Filter.pdf.

12 OpenNet Initiative (2004), 'A starting point: legal implications of internet filtering', accessed 19 December 2016, https://opennet.net/docs/Legal_Implications.pdf

13 For example, the 2000 European Parliament Directive on electronic commerce on hosting article 14 (1) obligates service providers to act expeditiously to remove or disable access to the information upon obtaining knowledge of illegal activity or information stored

For the purpose of filtering and blocking child sexual abuse content, Internet Service Providers do not only rely on rating systems to determine the suitability of a content site or a document. ISPs however, do implement content filtering blocking policies based upon information obtained from law enforcement, states and other parties working to reduce the availability of child sexual abuse material online. How this information is used depends on the filtering and blocking policies deployed by the respective party, e.g. the Internet Service Providers themselves.[14]

Filtering and blocking policies and mechanisms broadly fall into three categories, namely: content filtering based on key words, URL-based filtering, and Hash matching. Internet Service Providers can use lists containing key words or search terms that are associated with child sexual abuse materials to filter such content. These lists are termed 'blacklists' and are often informed by input from law enforcement agencies indicating which terms are used by child sex offenders or which are likely to be linked to child sexual abuse materials.[15]

Research shows that end users are increasingly relying on text and key word-based search tools to locate information of potential interest.[16] Offenders tend to begin their search using broad terms, such as 'porno', that are eventually refined to target specific content, using terms or acronyms like PTHC (preteen hardcore) or 'boylover'.[17] A clear understanding of the meaning of such acronyms and knowledge of the use of seemingly innocent words to refer to child sexual abuse or related conduct is necessary before including them on filtering lists, particularly when these same words are also used to describe innocent or lawful things. The challenge is to keep these lists updated to ensure they reflect reality and do not contribute to over- or under-blocking.

When someone enters a term using an online search tool or engine, it triggers a search in an existing indexing database, and returns a list of pointers to documents of potential interest for users to navigate and retrieve the content.[18] When keywords have been defined and keyword blocking is enabled, Internet Service Providers will implement software to block the sites containing a blacklisted keyword.[19]

Filtering and blocking can also be carried out by using a list or a database with URLs (Internet addresses) or domains hosting illegal content.[20] These lists apply national legislation and reflect national standards in relation to factors such as the age of the victim and type of offence depicted. Different parties provide lists of domains and/or URLs to Internet Service Providers and industry to limit the distribution of child sexual abuse material in their network.

For example, INTERPOL provides the 'worst of' list of domains containing the most severe child sexual abuse material according to defined criteria.[21] It is constructed and updated regularly in cooperation with national law enforcement agencies providing URLs that for example, have come up in investigations or were reported

at the request of a recipient of the service. The 2011 European Parliament Directive on combating the sexual abuse and sexual exploitation of children and child pornography article 25 includes an obligation for Member States to ensure that child pornography sites hosted within their territory are promptly removed […] and they have the possibility to block access to these sites in their territory. Information retrieved from European Parliament,"Directive on electronic commerce", *Official Journal of the European Union* L 178 (17 July 2000),1-16 and European Parliament, "Directive on combating the sexual abuse and sexual exploitation of children and child pornography", *Official Journal of the European Union* L 335 (17 December 2011).

14 Massarani, Leonardo C. (2002), "Content-indexing search system and method providing search results consistent with content filtering and blocking policies implemented in a blocking engine".

15 Steel, C.M.S. (2015) "Web-based child pornography: The global impact of deterrence efforts and its consumption on mobile platforms".

16 *Ibid.*

17 *Ibid.*

18 Massarani, Leonardo C. (2002), "Content-indexing search system and method providing search results consistent with content filtering and blocking policies implemented in a blocking engine".

19 Websense (2015), "Filtering based on keyword," *Web Security Help*, Triton (2015, v. 7.5), 207-208, accessed 10 March 2015, http://www.websense.com/content/support/library/web/v75/triton_web_help/triton_web_help.pdf.

20 Internet Watch Foundation (2015), "Emerging patterns and trends reports #1 Youth-produced sexual content," IWF in partnership with Microsoft, accessed 12 March 2015 https://www.iwf.org.uk/assets/media/resources/Emerging%20Patterns%20and%20Trends%20Report%201%20-%20Youth-Produced%20Sexual%20Content.pdf.

21 See http://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking/Criteria-for-inclusion-in-the-Worst-of-list for information on the criteria for inclusion in INTERPOL's Worst of-list. The fact that this list only includes the 'worst-of' type of material does

through hotlines and which have been assessed to contain child sexual abuse material.[22]

Other stakeholders such as CIRCAMP[23], the National Center for Missing and Exploited Children (NCMEC) [24] and the Internet Watch Foundation[25] operate similar lists which are implemented by Internet Service Providers and other industry partners in their networks. When a user tries to access one of the URLs or domains on the list, access will be blocked and the user will be redirected to an error page (404-page) or a splash page.

Finally, child sexual abuse content can be blocked by using databases of hashes[26] to match images that are known to be illegal. This works by means of an image matching technology called 'PhotoDNA'. PhotoDNA creates a unique signature, i.e., a numerical value for a digital image. This signature, like a fingerprint, can be compared with the signatures of other images to find copies of that image.[27] Child sexual abuse materials which are confiscated or encountered online can be matched against databases of hashes from known child sexual abuse images to distinguish and flag harmful images.

Once identified or filtered out, the images can be prevented from being accessed or shared, for example by means of blocking. These sets of hashes are shared with Internet Service Providers and Social Network sites by governments, law enforcement and different organisations. For example, Thorn[28] collaborated with Facebook, Google and six other technology industry companies to create the Industry Hash Sharing Platform. This was the first collaborative industry initiative to improve and accelerate the identification, removal and reporting of child sexual abuse images across different digital networks, using hash technology.[29] The system has since been transferred to the NCMEC.

The PhotoDNA technology only works for copies of child sexual abuse material which have already been identified and included in hash-databases. New or unseen child sexual abuse material will not be recognised through this filtering method, limiting its effectiveness in terms of filtering and blocking of all available child sexual abuse content online.

Different filtering schemes can thus be applied to sift out and block child sexual abuse content online at different levels. It is important to note that these methods only address material available and searched for on the surface web, or the part of the World Wide Web indexed by search engines. General blocking policies do not impact the hidden parts of the Internet. As more and more offenders move into secure environments, such as the Darknet, to exchange and access child sexual abuse material, filtering and blocking strategies will fail to affect large portions of content hosted and exchanged online.

---

not imply that websites not included in the list or other domains containing less-severe child sexual abuse material are necessarily legal to access in every country. In most countries a child is legally defined as anyone younger than 18, and (certain) acts related to images or films depicting a child in a sexual context are punishable by law. Typically, content is filtered and blocked by applying national legislation and national standards which can differ from and complement filtering efforts based on the worst of-list.

22 INTERPOL, "Access blocking: Criteria for inclusion in the Worst of List", accessed 10 March 2015, http://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking/Criteria-for-inclusion-in-the-Worst-of-list accessed 03/10/2015.

23 CIRCAMP is an abbreviation for Cospol [Comprehensive Operational Strategic Planning for the Police] Internet Related Child Abusive Material Project, initiated by the council of the national heads of police in Europe (EPCTF). It introduced the Child Sexual Abuse Anti Distribution Filter (CSAADF) and shares it with any law enforcement agency to block child sexual abuse material at domain level.

24 NCMEC operates the URL Initiative, thereby providing the Internet industry with a list of URLs for active Web pages containing apparent child sexual abuse material. Information retrieved from NCMEC (2015), "Voluntary Industry Initiatives", accessed 11 March 2015, http://www.missingkids.com/Exploitation/Industry.

25 The Internet Watch Foundation (IWF), the UK Hotline for reporting criminal online content, passes details of every identified non-UK website to the partner Hotline in that country. National and international enforcement agencies and INHOPE hotlines may also access the list on a mutual exchange basis. Information accessed on IWF (2015), "URL list", accessed 12 March 2015, https://www.iwf.org.uk/members/member-policies/url-list.

26 NCMEC (2015), "Photo DNA", accessed 12 March 2015, www.missingkids.com/Exploitation/Industry.

27 *Ibid.*

28 Thorn is an international non-governmental organisation focused on driving technology innovation to fight sexual exploitation of children.

29 Thorn (2015), "Industry Hash Sharing Platform", accessed 10 March 2015, https://www.wearethorn.org/reporting-child-sexual-abuse-content-shared-hash/.

These hidden environments offer a level of privacy and anonymity for offenders and enable a more secure exchange of child sexual abuse content over the Internet. With the volume of content in circulation having amplified in recent years, and seeing both the increasing trend of images and videos with infants and toddlers, and depicting greater violence than before, this constitutes a major concern.[30] Filtering and blocking only the 'public' content online is not sufficient to provide an effective response to the issue of online child sexual exploitation; however, it does dramatically reduce the amount of child sexual abuse material accessible on the public web.[31] Therefore it is a useful component of a broader approach to child sexual abuse content.

CONTENT AND FUNCTIONALITIES OF SPLASH PAGES RELATED TO CHILD SEXUAL ABUSE MATERIAL

After Internet Service Providers filter and block child sexual abuse content online by implementing the list of domains, key words or hashes in their networks, traffic from Internet users may then be redirected to a 'stop page' or splash page rather than the desired content. Some Internet Service Providers use error messages or 404-messages that will come up when access is denied to the user without providing additional information as to why and how access is blocked. Such messages usually contain the following sentence: "file not found or removed".

Splash pages provide deterrence messages to users as a complementary measure to just restricting access to specific online content, offering additional information. The information, as well as the tone in which messages are provided, differ per splash page and can be designed to reflect the situation in a specific country. For instance, some pages enter the number of a local hotline that the Internet Service Providers works with. CSAM-related splash pages usually contain one or more of the following messages and information:

- Stating the fact that access is denied (error or 404-report);
- Reason for why access was blocked, e.g. "you are trying to access illegal material";
- Information, referral and contact details of institutions providing help for people who are struggling with (or who know persons struggling with) a sexual preference for minors and children, or with deviant online behaviour;
- Information with respect to local/national/international law enforcement;
- Texts about or links to relevant legislation on child sexual abuse image offences;
- Information on where to direct complaints about particular content being blocked;
- Information and/or links to hotlines to report child sexual abuse material online; or,
- (General) information or links to information on child sexual abuse material.

Information on a splash page is visible to anyone who triggers a filtering and blocking system through his or her online behaviour. By showing a splash page rather than the desired illegal content, does not only obstruct offenders in their attempts to access child sexual abuse content, it also prevents unwanted exposure to such illegal content for the general Internet population. People landing on a deterrence splash page may be potential, first-time, or repeat/experienced offenders. They may also be people who have no intention to commit offences related to child sexual abuse images, but happen to display certain behaviours that automatically (right or wrong) alert filtering and blocking systems.

Trying to open a web page on a domain defined to contain child sexual abuse material may not always be an intentional act, but can also be the result of 'not thinking', criminal hijacking of the person's account, or the splash page showing up as a result of over-blocking. Accessing a domain with child sexual abuse material does

30 NetClean (2016), "The NetClean Report 2016", 13, accessed 21 December 2016, https://www.netclean.com/the-netclean-report-2016; EUROPOL (2016), "The Internet Organised Crime Threat Assessment (IOCTA) 2016", 6, accessed 21 December 2016, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016.

31 INTERPOL (2015), "Access blocking: the INTERPOL Worst-of list"; accessed 10 March 2015. http://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking/The-INTERPOL-%22Worst-of%22-list.

not necessarily prove criminal intent.[32] People could be trying to find information concerning child sexual abuse images for other reasons than abuse, such as seeking help for themselves or for relatives. Based on this understanding, it is important to consider the various ways in which the information provided in different splash pages might affect different users.

Building knowledge

Splash pages can contain information stating that the conduct of the Internet user is illegal. For example, the INTERPOL splash pages showing in response to URL-queries on the 'worst-of'-list state the reason for redirection and links to the relevant legislation.[33]

Most offenders looking for child sexual abuse material for the first time do so via surface web-based search engines.[34] It is possible that some of these users are not fully aware that such searches are illegal and a message stating this type of information may act as a deterrent for them. Having a mechanism – albeit a splash page – provide a direct message on the computer screen saying that it is not normal, acceptable and/or illegal to conduct this behaviour might function as a wakeup call. Quayle and Taylor (2015) argue that more messages highlighting the negative impact of child sexual abuse images will reduce the normalisation of the act of viewing or accessing material.[35] Following that theory, messages that emphasise the potential consequences of such behaviours could then function as deterrence.

Conversely, it is important to acknowledge that notifying or informing offenders by means of splash pages does not necessarily result in them stopping their behaviours. It might in fact, encourage them to be more careful and take more informed actions when trying to access such materials online, potentially leading to them moving away from more amateuristic searches on the surface web to the more hidden parts of the Internet. Although this could imply that less child sexual abuse material would be (easily) available on the surface web, it does not mean that there would be less child sexual abuse material in circulation online, in general. Additionally, offenders moving away to hidden parts of the Internet would negatively influence offender identification opportunities for follow up investigations and for obstructing them in their actions.

Installing the feeling of risk in offenders

Splash pages can also include information on the related penalties for child sexual abuse material conducts. Messages about the severity of punishment may influence behaviour if potential offenders weigh up the consequences of their actions and conclude that the risks of punishment are too severe.[36] Research by Wright (2010) shows that messages indicating a risk of apprehension are generally more effective in terms of deterrence than information on the severity of punishment. In the past, Thorn used to deploy the following message stressing that risk of apprehension: "We know where you are: if we can find you, so can the police". Similarly, increasing the certainty of punishment has demonstrated to be more likely to produce deterrent benefits than the severity of the punishment.[37]

Although installment of fear may have a deterrent effect in terms of scaring users away, Thorn states that they have also witnessed users quickly moving away from any pages that include fear based messaging and not engaging with the page at all.[38] Thorn pointed out that according

---

32 Ibid.

33 Ibid.

34 Steel, C.M.S. (2015) "Web-based child pornography: The global impact of deterrence efforts and its consumption on mobile platforms", 5.

35 Quayle, E and Tailor, M. (2015), "Child pornography and the Internet, perpetuating a cycle of abuse, Deviant Behavior, 23 (4), 331-361 quoted in Steel C.M.S. (2015), "Web-based child pornography", Child Abuse & Neglect (2015), 5.

36 Wright, Valerie (2010), "Deterrence in Criminal Justice: evaluating certainty vs. severity of punishment", The Sentencing Project, 2, accessed 18 March 2015, http://www.sentencingproject.org/doc/Deterrence%20Briefing%20.pdf.

37 Nagin, Daniel and Pogarsky, Greg (2010), "Integrating Celerity, Impulsivity, and Extralegal Sanction Threats into a Model of General Deterrence: Theory and Evidence," Criminology, 39(4), 2001 quoted in Wright, Valerie "Deterrence in criminal justice: evaluating certainty versus severity of punishment", The Sentencing Project, 4, accessed 18 March 2015, http://www.sentencingproject.org/doc/Deterrence%20Briefing%20.pdf

38 Treitman, Leah, Thorn, telephone conversation with ECPAT International, Bangkok, Thailand, 2 April 2015.

to psychologists, fear alone is not a sustainable measure for substantial behavioural change in the long run.[39] If deterrence messaging aims to induce behavioural change, both a long-term engagement and an offer to help perpetrators is necessary.

Offering help

Some users confronted with a splash page might be intentionally looking for child sexual abuse material, yet not wanting to engage in this type of behaviour. They might be dealing with feelings of guilt, shame or fear, and may be aware of the illegality and potential repercussions of such behaviour for themselves or the victims. By offering information on where (potential) offenders can find support, a user is provided with an easy tool to seek help instead of continuing his or her behaviour.

For example, Thorn uses prevention messages encouraging people to seek help through resources, including Stop it Now!'s confidential helpline.[40] When Internet users search for this type of material, they receive an ad bringing them to a splash page with information about the illegality of viewing child sexual abuse material and resources for people struggling with a sexual preference for minors and children. This includes statements such as: "Sexually attracted to children? Understanding people are ready to help".

Offenders might not even know that such resources are available, or where to find them. They may also be reluctant to reach out because of a fear of the consequences. Stop it Now! US indicate that they receive visits to their website from between 200 and 250 people a month as a result of Thorn's splash pages.[42] Thorn further states that of the intercepted individuals more than 13% sought more information about receiving help, which accounts for more than 17,000 people.[42] Both Thorn and Stop it Now! stress that it is important to include help information in any deterrence message that is also targeting behavioural change. Such behavioural change can start with a deterrence message, but requires to be complemented and effectuated by continued engagement with those seeking help.[43]

Encouraging to report on child sexual abuse material online

Information about the responsibility and possibility for the general public to report when confronted with child sexual abuse material online can also be included on splash pages. By providing this information in combination with links to reporting websites or instruments, people are facilitated or motivated to use these reporting tools. This can result in more reports of online child sexual abuse content, eventually decreasing its availability online as these reports should be followed up by filtering and blocking content.

INTERPOL believes that blocking child sexual abuse material in as many networks and countries as possible will dramatically reduce the customer base of child sexual abuse content providers; perhaps to a point where it will no longer be a lucrative business.[44] Consequently, getting more Internet users to report when encountering child sexual abuse material online will ultimately make it more difficult for offenders to find available content online again, thus providing an additional deterrence benefit.

---

39 Treitman, Leah, Thorn, telephone conversation with ECPAT International, Bangkok, Thailand, 2 April 2015.

40 Treitman, Leah, Thorn, E-mail communication with ECPAT International, Bangkok, Thailand, 3 December 2015.

41 Coleman, Jenny, Stop it Now! US, E-mail communication with ECPAT International, Bangkok, Thailand, 10 March 2015.

42 Thorn (2015), "Deterrence programs to prevent child sexual exploitation," accessed 20 March 2015, https://www.wearethorn.org/deterrence-prevent-child-sexual-abuse-imagery/.

43 Treitman, Leah, Thorn; Coleman, Jenny, Stop it Now! US, telephone conversation with ECPAT International, Bangkok, Thailand, 2 April 2015.

44 INTERPOL, "Access blocking: Information for ASPs".

45 For example, the Universal Declaration of Human Rights (article 19) and the Declaration on Freedom of Opinion and Expression. Information retrieved from United Nations (2010), "The Universal Declaration of Human Rights", accessed 17 March 2015 http://www.un.org/en/documents/udhr/index.shtml#a19 and UN et al. (2011), "International mechanisms for Promoting Freedom of Expression: Joint Declaration of Freedom of Expression and the Internet", June 2011, accessed 17 March 2015.

46 United Nations Economic and Social Council (2000), "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (E/CN.4/2000/63)," January, Fifty-sixth session, 15, accessed 17 March 2015. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G00/102/59/PDF/G0010259.pdf?OpenElement.

Creating transparency about filtering and blocking measures

Since any filtering and blocking measure is about restricting access to information, it is important to include information on the splash page explaining why information is blocked. This provides a necessary level of transparency for the user since restricting access to content often conflicts with both the freedom of expression and the freedom of access to information, unless it follows (international) law. These freedoms are safeguarded by means of different national and international laws and frameworks.[45] Users are entitled to be informed about decisions to restrict access.

The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression urges governments to review or adopt legislation requiring that any refusals to requests for information should accompany substantive written reasons for the refusal(s), in line with the public's right to receive information.[46]

In the UN Joint Declaration on freedom of expression and the Internet, Article 3, principle (c) states that products designed to facilitate end-user filtering should be required to be accompanied by clear information to end-users about how they work and the potential pitfalls in terms of over-inclusive filtering.[47] INTERPOL also believes users should be provided with an explanation as to why their access is restricted. The purpose is to increase transparency and to enable the affected person to request a review and re-evaluation.[48] This information can be included in splash pages.

Providing tools to object to mis-blocking

Finally, the opportunity to request a review or re-evaluation of blocked content is important because of the risk of over-blocking or restricting access to information that should be available to the public. The process of filtering usually works automatically by using certain indexes of words, URLs, domains or hashes. Since this process is automated it is very difficult to apply nuances to filter out those users, attempts or content that might correspond with the programmed databases or 'blacklists', but which do not actually refer to child sexual abuse material online.[49]

Many blacklists will contain websites or content incorrectly classified as 'undesirable content' because it is automatically categorised without regard to its context or meaning.[50] For example, a human rights organisation page was blocked for being 'sexually explicit' due to the keyword filtering mechanism detecting the words 'at least 21' in a sentence that referred to a number of people who were killed or wounded as a result of shootings.[51]

Legal content might thus be wrongfully filtered out and blocked, thereby impacting a users' right to freedom of expression and information. There are legal acts and directives in place focusing on the issue of (judicial) redress.[52] In addition, some splash pages provide information to file complaints or appeals against the accuracy of an assessment. For example, the stop page from INTERPOL includes information on a procedure to file a complaint, and the Internet Watch Foundation encourages hotlines and others to include information for appeal.[53] This

47 UN, OSCE, OAS, ACHPR, "Joint Declaration".

48 INTERPOL, "Access blocking: Information for ASPs".

49 Chen Ding et al. (1999) "Centralized content-based Web filtering and blocking: how far can it go?" Systems, Man and Cybernetics. 1999, (vol. 2) 115-119, accessed 10 March 2015 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=825218&isnumber=17632.

50 Heins, Marjorie and Cho, Christina (2006), "Internet Filters: A Public Policy Report", Free Expression Policy Project, accessed on 9 November 2015, http://ncac.org/wp-content/uploads/import/Internet%20Filter.pdf.

51 Haselton, Bennett (2000), "Amnesty Intercepted: Global human rights groups blocked by Web censoring software", accessed on 11 October 2015, http://www.peacefire.org/amnesty-intercepted/.

52 For example, the directive of the European Parliament on combating the sexual abuse and sexual exploitation of children and child pornography, Article 25 (2) states that "measures taken by member states to block access to web pages containing or disseminating child pornography [...] must be set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that the users are informed of the reason for the restriction. Those safeguards shall also include the possibility of judicial redress". Information retrieved from European Parliament (2011), "Directive on combating the sexual abuse and sexual exploitation of children and child pornography". Official Journal of the European Union L 335 (17 December 2011), 1-14; accessed 11 March 2015. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0093&from=EN.

53 IWF, "URL list".

information allows users to act on their right to freedom of expression and information and provides a tool to regain access to legal content if it complies with the law.

CONCLUSION: SPLASH PAGES AS JUST ONE ELEMENT IN A HOLISTIC APPROACH

The aforementioned functionalities of splash pages provide added value to traditional deterrence schemes involving only filtering, blocking and stop pages. It is clear that different types of information could have varying types and degrees of impact upon the Internet users who are faced with the splash page. Offenders might be deterred from continuing or expanding their attempts to access child sexual abuse material, upon realising and recognising that their behaviour is illegal; that there will be (legal) consequences if apprehended; that they are neither invisible nor intangible when conducting illegal behaviour online; and that there are easily accessible means for seeking help to deal with their deviant online behaviour. Moreover, the general Internet population might have a better understanding of the issue of child sexual abuse material, be encouraged to report such content and have a means to protect their freedom of expression and information where content is believed to be improperly blocked. All of these functionalities and potential impacts diminish however, when websites deploy a stop-page or error-message instead of using both splash pages that contain all or some of the information highlighted.

At the same time, it is important to acknowledge the shortcomings of deterrence schemes including filtering and blocking policies and splash pages. They might drive offenders to the hidden parts of the Internet where identification is difficult and child sexual abuse material can be shared with little chance of offenders being apprehended.

Splash pages can also lead to over-blocking. To avoid over-blocking it is important to make sure filtering and blocking procedures, as well as the accompanying splash pages are carefully designed and regularly updated based on lessons learned, redress-reports and law enforcement information. Additionally, measures meant to restrict access – whether stop pages or splash pages – should always be complemented with information about why content is being blocked as well as information to redress that decision to ensure transparency and respect of the right to information.

Concerning the other potential functionalities of splash pages – building knowledge; installing a feeling of risk for offenders; offering help – it is necessary to acquire a better understanding of the impact of splash pages on different kinds of Internet users, and child sex offenders in particular. Although some data has demonstrated that splash pages indeed can influence people's behaviours, for example by seeking help, we cannot assume that just any information will have a (long-term) deterrence effect on those deliberately trying to access or share child sexual abuse content.

Offenders attempting to access child sexual abuse material do not represent a homogenous group, but rather, are people with different motivations, backgrounds, experiences and perceptions on child sex offending. Regardless of the content of any deterrence message, there will be offenders unaffected in their pursuit however; there might be (first-time) offenders susceptible to messages installing fear of apprehension. Some users might be encouraged to move to the hidden parts of the Internet, while others take advantage of the help lines offered to them.

To understand what works it is important to conduct research on user behaviour online after being faced with a splash page. For example, it could be interesting to see responses to different kind of messages, especially if this could be monitored for the same user/IP-address.

Organisations deploying splash pages to restrict access to child sexual abuse material could be a great source of information in understanding the effectiveness and reach of such measures. Additionally, discussing the issue of deterrence with known child sex offenders who might be willing to share their thoughts on what messages potentially would have stopped them in their endeavors could be of real added value for future deterrence messaging.

Considering the fact that child sex offenders are a diverse group of people, it would likewise be beneficial to explore opportunities to target users with appropriate deterrence messages matching their profile. It may be possible to

add various factors in a filtering scheme to differentiate between searches unmistakably referring to child sexual abuse materials and more amateurish searches. For example, the former may use (very) specific search terms while attempting to conceal behaviour; this might inform a profile indicating the level of experience, knowledge or simply coincidence. Or else, a user's IP-address could be flagged and logged to determine who/which IP-address is attempting to access child sexual abuse material repeatedly. This profile information in turn, could inform the type of message best paired with either the offender or the offender's specific type of behaviour.

Although some privacy activists disagree, the use of splash pages is a mild measure in the approach against child sexual abuse online as it only affects the availability and access of child sexual abuse materials on the surface web, but does not have any impact on content exchanged in the hidden parts of the Internet. As more and more child sex offenders are deploying anonymising tools and platforms to access and share illegal content, it is important to acknowledge that splash pages, regardless of the content, will only affect a fragment of the offender population online.

Additionally, the different filtering and blocking methods applied do not filter out all of the illegal content uploaded, shared or accessed online. For example, filtering by means of PhotoDNA only sifts out those images that have already been seen and classified as child sexual abuse content and which have been integrated in the hash sets. Since these hash sets also work for images that have been slightly altered – such as being cropped – this means that Internet users will be well protected from unwanted encounters with such content.

However, new or formerly unseen child sexual abuse material is not recognised and filtered out through this filtering method. As these new materials could depict recent or current instances of child sexual abuse and exploitation, they therefore require quick identification.

To conclude, although it is worthwhile to look into the effectiveness and potential broader application of splash pages, it remains important to consider the application of splash pages and wider deterrence schemes as just one measure in a broader approach to child sex offenders online. Filtering and blocking restricts availability of child sexual abuse content on the surface web, but does not affect material exchanged in different parts of the Internet. It does not by itself remove material that is present on the Internet or touch on the root causes of child sexual abuse behaviours.

Although some information provided in splash pages might resonate with certain offenders, potentially leading to long-term positive results, many offenders will not be so easily deterred in their tracks. Therefore, research into understanding and optimising the effectiveness of splash pages is necessary in order to improve deterrence schemes' preventive and restrictive impact.

Ultimately, blocking access to child sexual abuse content prevents re-victimisation of the children depicted (through re-use of the materials), protects the general Internet public from unwanted exposure to such illegal content, and makes it more difficult for offenders to access child sexual abuse pictures, videos and other materials. However, considering the limitations of filtering, blocking and splash pages measures, this should always be considered as just one element in a holistic approach to online child sexual exploitation.

BIBLIOGRAPHY

Chen Ding *et al*. (1999), "Centralized content-based Web filtering and blocking: how far can it go?" *Systems, Man and Cybernetics (vol. 2) 115-119, accessed 10 March 2015.* http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=825218&isnumber=17632.

European Parliament (2000), "Directive on electronic commerce". *Official Journal of the European Union* L 178 (17 July 2000), 1-16; accessed 11 March 2015. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML.

– – – (2011), "Directive on combating the sexual abuse and sexual exploitation of children and child pornography". *Official Journal of the European Union L 335 (17 December 2011), 1-14; accessed 11 March 2015.* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0093&from=EN.

EUROPOL (2016), "The Internet Organised Crime Threat Assessment (IOCTA) 2016", accessed 21 December 2016, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016.

Haselton, Bennett (2000), "Amnesty Intercepted: Global human rights groups blocked by Web censoring software", accessed 11 October 2015, http://www.peacefire.org/amnesty-intercepted/.

Heins, Marjorie and Christina Cho (2006), "Internet Filters: A Public Policy Report", *Free Expression Policy Project, accessed 9 November 2015,* http://ncac.org/wp-content/uploads/import/Internet%20Filter.pdf.

Internet Watch Foundation (IWF) (2015), "Emerging patterns and trends reports #1 Youth-produced sexual content," IWF in partnership with Microsoft, accessed 12 March 2015 https://www.iwf.org.uk/assets/media/resources/Emerging%20Patterns%20and%20Trends%20Report%201%20-%20Youth-Produced%20Sexual%20Content.pdf.

––– (2015), "URL list"; accessed 12 March 2015. https://www.iwf.org.uk/members/member-policies/url-list.

INTERPOL (2015), "Access blocking: Information for ASPs", accessed 10 March 2015. http://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking/Information-for-ASPs.

– – – (2015), "Access blocking: Criteria for inclusion in the Worst of List", accessed 10 March 2015. http://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking/Criteria-for-inclusion-in-the-Worst-of-list accessed 03/10/2015.

– – – (2015), "Access blocking: the INTERPOL Worst-of list"; accessed 10 March 2015. http://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking/The-INTERPOL-%22Worst-of%22-list.

KG Blog, (n.d.), "Flash pages"; accessed 6 March 2015. https://www.karelgeenen.nl/termen/splash-page/.

Kim, H., Coyle J.R. and Gould, S.J. (2009), "Collectivist and Individualist Influences on Website Design in South Korea and the U.S.: A Cross-Cultural Content Analysis", *Journal of Computer-Mediated Communication: 14, 581-601.*

Lennartz, Sven (n.d.), "Splash pages: do we really need them?" Smashing Magazine; accessed 9 March 2015. http://www.smashingmagazine.com/2007/10/11/splash-pages-do-we-really-need-them/.

Massarani, Leonardo C. (2002), "Content-indexing search system and method providing search results consistent with content filtering and blocking policies implemented in a blocking engine." *Armonk, New York: International Business Machines Corporation; accessed 10 March 2015.* https://docs.google.com/viewer?url=patentimages.storage.googleapis.com/pdfs/US6336117.pdf.

Nagin, Daniel and Pogarsky, Greg (2010), "Integrating Celerity, Impulsivity, and Extralegal Sanction Threats into a Model of General Deterrence: Theory and Evidence," *Criminology, 39(4), 2001 quoted in Wright, Valerie "Deterrence in criminal justice: evaluating certainty versus severity of punishment", The Sentencing Project, 4, accessed 18 March 2015,* http://www.sentencingproject.org/doc/Deterrence%20Briefing%20.pdf.

NCMEC (2015), "Photo DNA"; accessed 12 March 2015. http://www.missingkids.com/Exploitation/Industry.

– – – (2015), "Voluntary Industry Initiatives"; accessed 11 March 2015. http://www.missingkids.com/Exploitation/Industry.

NetClean (2016), "The NetClean Report 2016", accessed 21 December 2016, https://www.netclean.com/the-netclean-report-2016.

OpenNet Initiative (2004), "A starting point: legal implications of internet filtering", accessed 19 December 2016, https://opennet.net/docs/Legal_Implications.pdf.

Palfrey Jr., John G. (2011), "Local Nets on a Global Network: Filtering and the Internet Governance Problem", in *The Global Flow of Information: Legal, social and cultural perspectives, eds. Subramanian, Ramesh and Eddan Katz, New York: NYU Press.*

Quayle, E and Tailor, M. (2015), "Child pornography and the Internet, perpetuating a cycle of abuse, Deviant Behavior, 23 (4), 331-361 quoted in Steel C.M.S. (2015), "Web-based child pornography", Child Abuse & Neglect (2015).

Steel, C.M.S. (2015), "Web-based child pornography: The global impact of deterrence efforts and its consumption on mobile platforms", Child Abuse & Neglect (2015): 1-9.

Thorn (2015), "Industry Hash Sharing Platform", accessed 12 March 2015. https://www.wearethorn.org/reporting-child-sexual-abuse-content-shared-hash/.

– – – (2015), "Deterrence programs to prevent child sexual exploitation", accessed 20 March 2015. https://www.wearethorn.org/deterrence-prevent-child-sexual-abuse-imagery/.

UN (2010), "The Universal Declaration of Human Rights"; accessed 17 March 2015. http://www.un.org/en/documents/udhr/index.shtml#a19.

UN, OSCE, OAS, ACHPR (2011), "International Mechanisms for Promoting Freedom of Expression: Joint Declaration on Freedom of Expression and the Internet"; accessed 17 March 2015.

UN Human Rights Council (2014), "Report of the Special Rapporteur on the sale of children, child prostitution and child pornography, Maud de Boer-Buquicchio", UN Doc. A/HRC/28/56, 22 December 2014, para. 67-68.

UN Economic and Social Council (2000), "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", (E/CN.4/2000/63). Fifty-sixth session, accessed 17 March 2015. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G00/102/59/PDF/G0010259.pdf?OpenElement.

Websense (2015), "Filtering based on keyword". *TRITON Web Security Help. San Diego, US: Websence Inc. v7.5 (2015). Accessed 10 March 2015.* http://www.websense.com/content/support/library/web/v75/triton_web_help/triton_web_help.pdf.

Wright, Valerie (2010), "Deterrence in Criminal Justice Evaluating Certainty vs. Severity of Punishment", *The Sentencing Project*, accessed 18 March 2015. http://www.sentencingproject.org/doc/Deterrence%20Briefing%20.pdf.

Online Child Sexual Abuse and Exploitation: Spotlight on Female Sex Offenders

By: Alessia Altamura

INTRODUCTION

With the advent and growth of the Internet, the use of information and communication technologies (ICTs) for child sexual abuse and exploitation[1] is receiving increased attention from researchers, policy makers and other professionals. Literature on Internet child sex offending has proliferated and so have programmes to address this crime.

However, most of these efforts have focused on male perpetrators while the role played by women in the commission of ICT-facilitated child sex offences has only been minimally acknowledged, thus remaining an understudied and marginalised topic in both academic and civil society circles.

Although limited in numbers, the cases of females offending online recently brought to light by the media in several countries, together with the scant research available investigating this specific thematic area, demonstrate that applying a gender lens to the analysis of Internet child sex crimes is an essential step toward the prevention and eradication of online child sexual abuse and exploitation. This article is an attempt to review current knowledge on female Internet sex offenders and deepen the understanding of this critical, yet neglected segment of the demand.

Drawing from a variety of sources including news media, this article explores the specificity of female online offending while also examining the potential similarities between male and female Internet sex offenders, as well as between women engaging in contact crimes and those offending online. Gaps in existing literature will also be highlighted and recommendations for future research and programming will be provided.

Although this article attempts to analyse some primary information, particularly from public databases of sex offenders established by NGOs or Internet watchdogs, it must be viewed essentially as a literature review whose conclusions warrant further substantiation from scientific research.

Studies collected and analysed include mainly journal articles retrieved through online searches on specialised databases (such as PsycINFO, Web of Science and Dissertations and Thesis Fulltext). The search terms used for this purpose include, among other: Internet, online, cyberspace, female sex offender, women, child pornography, child abuse materials, grooming, live web streaming, non-contact offenders, solo offender, and co-offender. The resources identified were accessed primarily by using Researchgate. Additional studies were also found by reviewing the reference lists of the initial studies and then utilising Google Scholar. The databases of sex offenders established by NGOs or Internet watchdogs were retrieved through a

1 The Interagency Working Group on Sexual Exploitation of Children defines: a) online child sexual abuse as "any form of sexual abuse of children, as set forth in the previous sections, which has a link to the online environment. Thus, online sexual abuse can take the form of, for instance, sexual molestation and/or harassment through social media or other online channels"; and b) online child sexual exploitation as "all acts of a sexually exploitative nature carried out against a child that have, at some stage, a connection to the online environment. It includes any use of ICT that results in sexual exploitation or causes a child to be sexually exploited or that results in or causes images or other material documenting such sexual exploitation to be produced, bought, sold, possessed, distributed, or transmitted. This notion can thus encompass (but is not limited to): - sexual exploitation that is carried out while the victim is online (such as enticing/manipulating/threatening a child into performing sexual acts in front of a webcam); - identifying and/or grooming potential child victims online with a view to exploiting them sexually (whether the acts that follow are then carried out online or offline); - the distribution, dissemination, importing, exporting, offering, selling, possession of, or knowingly obtaining access to child sexual exploitation material online (even if the sexual abuse that is depicted in the material was carried out offline)." See Interagency Working Group on Sexual Exploitation of Children (2016), "Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse", Bangkok: ECPAT International and ECPAT Luxembourg, 22 and 27-28.

Google Search. A search for online news reports was also undertaken, including media articles in local languages that were translated using online translation tools (mainly "Lexicool").

The scant availability of research on the topic of female Internet sex offenders mostly based on very small samples, coupled with the difficulty in accessing official records on this offender population, not to mention the limitations implicit in using media reports or other unofficial sources of information (such as NGO databases of sex offenders), hinder the validity of the findings from this review which should is in no way conclusive, representational or generalisable.

WHAT IS THE PREVALENCE OF FEMALE INTERNET SEX OFFENDING?

One of the motivations behind the limited consideration given to the use of ICTs by women to perpetrate sex offences against children, is linked to its low prevalence. The fact that only a small proportion of females are detected, arrested or convicted for online child sexual abuse and exploitation has fuelled the belief that this problem is so uncommon to become virtually non-existent.[2]

While this perception seems to be widespread, the real prevalence of women committing child sex crimes in cyberspace remains unknown and difficult to measure. As observed with other forms of child sexual exploitation, there are a number of challenges and issues relating to data collection and reporting making it hard, if not impossible, to provide accurate estimates.

First, studies based on law enforcement information will usually indicate negligible rates of female perpetrators due to difficulties in detection of online offences generally and female sex offending in particular. Second, victims of online child sex crimes committed by women may face barriers to reporting such as fear of stigma, shame, and lack of reporting mechanisms.[3] Third, the absence of harmonised definitions of child sexual abuse material and Internet-related child sex crimes across countries, combined with the lack of data collection systems disaggregating information based on gender, hinders efforts to accurately report prevalence. Fourth, statistics often refer to small samples and are limited in geographic scope in that they are only available in few Western countries primarily affected by online child sexual abuse and exploitation, while figures relating to regions that are now identifying an emerging problem (e.g. Africa and Asia) are still lacking.

In the absence of quantitative research looking specifically at the ratio of female-to-male Internet child sex offending, Table 1 offers a snapshot of prevalence rates for incidents of ICT-facilitated child sex crimes carried out by women from publically available studies.

Table 1. Prevalence rates for incidents of ICT-facilitated child sex crimes carried out by women.

Study/Source	Country	Type of sexual crime	Sample/Type of data	Proportion female
Alexy, Burgess and Baker (2005)[i]	USA	Trading child sexual abuse material	Cases published in news media	5.3%
Wolak, Mitchell and Finkelhor (2005)[ii]	USA	Possessing child sexual abuse material	Arrests reported by law enforcement agencies	<1%
Seigfried, Lovely and Rogers (2008)[iii]	USA	Consumption of child sexual abuse material	Respondents to online survey	5.5%

2 Elliott, Ian A., Ashfield, Sherry (2011), "The use of online technology in the modus operandi of female sex offenders", *Journal of Sexual Aggression* 17, n. 1 (2011): 2. The next section of this article covers in depth the issue of gender stereotyping and the role gender perceptions play in child exploitation.

3 The next section of this article covers in depth the issue of gender stereotyping and the role gender perceptions play in child exploitation. New Zealand Department of Internal Affairs (2007), "Internet traders of child pornography: profiling research – update", accessed 9 November 2016, https://www.dia.govt.nz/pubforms.nsf/URL/InternetTradersOfChildPornography-ProfilingResearchUpdate-February2007.pdf/$file/InternetTradersOfChildPornography.

Study/Source	Country	Type of sexual crime	Sample/Type of data	Proportion female
Babchishin, Hanson and Hermann (2011)[iv]	Australia, France, Germany, New Zealand, Switzerland, the Netherlands, Canada and the United States	Online child sexual abuse and exploitation	27 different samples/ convictions, arrests, charges and self-report	<3%
CEOP (2013)[v]	UK	Production of child sexual abuse material	Child abuse images collected	24% of the images of child abuse analysed, depicted sexual contact between a child and an adult female
Seigfried-Spellar (2013)[vi]	United States, United Kingdom, Australia, and Canada	Consumption of child sexual abuse material	Respondents to online survey	18.7%
Wolak, Mitchell and Finkelhor (2014)[vii]	USA	Aggressive sexual solicitation	Youth interviewed by telephone	16%
Leukfeldta, Jansenb and Stolc (2014)[viii]	Netherlands	Child sexual abuse material	Police files	<2%
NSPCC (2015)[ix]	UK	Online child sexual abuse and exploitation	Convictions	<2%
Schulz et al. (2016)[x]	Germany, Sweden and Finland	Sexual solicitation of minors	Respondents to online surveys	Soliciting adolescent: 30.6%; soliciting child: 17.2%

i Alexy, Eileen M., Burgess, Anna W. and Baker, Thomas (2005), "Internet offenders: traders, travelers, and combination trader–travellers", Journal of Interpersonal Violence 20, n. 7 (2005): 804-12.

ii Wolak, Janis, Mitchell, Kimberly and Finkelhor, David (2005), "Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study", National Center for Missing and Exploited Children: USA, 2, accessed 9 November 2016, http://www.unh.edu/ccrc/pdf/jvq/CV81.pdf.

iii Seigfried, Kathryn C., Lovely, Richard W., and Rogers, Marcus K. (2008), "Self-reported online child pornography behaviour: A psychological analysis", International Journal of Cyber Criminology 2, n. 1 (2008): 286-297, accessed 9 November 2016, http://www.cybercrimejournal.com/Seigfriedetalsijccjan2008.htm.

iv Babchishin, Kelly M., Hanson, Karl R., and Hermann, Chantal A. (2011), "The characteristics of online sex offenders: A meta-analysis", Sexual Abuse: A Journal of Research and Treatment 23, n.1 (2011): 95.

v Child Exploitation and Online Protection Center (2013), "Threat Assessment of Child Sexual Exploitation and Abuse 2013", London: CEOP, 9, accessed 9 November 2016, https://www.ceop.police.uk/Documents/ceopdocs/CEOP_TACSEA2013_240613%20FINAL.pdf.

vi Seigfried-Spellar, Kathryn (2013), "Individual Differences of Internet Child Pornography Users: Peculiar Findings in a Community-Based Study", International Journal of Cyber Criminology 7, n. 2 (2013): 146.

vii Wolak, Janis et al. (2014), "Trends in Unwanted Online Experiences and Sexting: Final Report. 2014", Durham, NH: Crimes against Children Research Center, accessed 9 November 2016, http://scholars.unh.edu/cgi/viewcontent.cgi?article=1048&context=ccrc.

viii Leukfeldta, Rutger E., Jansenb, Jurjen and Stol, Wouter P. (2014), "Child pornography, the Internet and juvenile suspects", Journal of Social Welfare and Family Law 36, n. 1 (2014): 7.

ix NSPCC, "Two sex offenders convicted a day for possession of child abuse images", 22 July 2015, accessed 9 November 2016, https://www.nspcc.org.uk/fighting-for-childhood/news-opinion/huge-scale-of-online-child-abuse-images-revealed/.

x Schulz, Anja et al. (2016) "Online Sexual Solicitation of Minors: How Often and between Whom Does It Occur?", Journal of Research in Crime and Delinquency 53, n.2 (2016): 177.

As these data demonstrate, research using information from the criminal justice system (e.g. arrests and convictions) indicates that the proportion of females engaging in illegal conduct does not rise beyond 3% of all incidents. Official records from several countries likewise confirm low prevalence. In New Zealand, for example, 2007 statistics reveal that only 1 in 215 offenders convicted for violating the country's censorship laws (i.e., possession or distribution of any sexualised images of children, images depicting torture, or images involving bestiality and necrophilia) was female.[4] In Texas, analysis of a public database shows that only 14 out of 1440 individuals placed on the Sex offenders' register for promotion and possession of child sexual abuse material were women.[5]

In contrast to police and judicial statistics, victimisation surveys and offenders' studies using self-reports point out significantly higher prevalence rates of female Internet child sex offending, ranging from over 5% for consumption of child sexual abuse material to over 30% for online solicitation of adolescents. However, as noted by Schulz et al. (2016), both law enforcement data and studies sampling victims may be biased; the former because they only capture cases reported and detected and the latter because 'the victims' perception may be wrong due to deception or fantasy play by the perpetrators".[6]

Although it is not possible to draw general conclusions from these figures, data on the prevalence rates regarding women seem to be partially consistent with findings on the frequency of female sex offending in general. A meta-analysis by Cortoni, Babchishin and Rat published in 2016, found that while the proportion of female sexual offenses reported to police is approximately 2%, this number increases to 12% in victimisation surveys.[7]

Besides the uncertainty regarding prevalence rates, there is no accurate information about current trends in Internet child sex offending by females. Nevertheless, some evidence of an increasing involvement of women in abuse and exploitation recently emerged. CEOP's 2012 and 2013 "Threat Assessment of Child Sexual Exploitation and Abuse", for example, registered a rise in the number of female producers of indecent images of child abuse.[8] Likewise, in its 2014 report, the Italian association Meter, a charity specialised in counteracting online child sexual abuse materials, raised concern over a 70% increase in the amount of infants abused by women in the depictions analysed.[9]

Whether this growing trend reflects a real rise in the number of female perpetrators abusing and exploiting children online remains unclear. While the general growth in the volume of child sexual abuse materials and Internet child sex crimes observed globally[10] may also concern female perpetrators, the rising numbers of incidents concerning women offending online may be due, among others, to increased awareness or reporting of female offending, better law enforcement or more effective cooperation in the fight against online child sex offences.

4 New Zealand Department of Internal Affairs (2007), "Internet traders of child pornography: profiling research – update", accessed 9 November 2016, https://www.dia.govt.nz/pubforms.nsf/URL/InternetTradersOfChildPornography-ProfilingResearchUpdate-February2007.pdf/$file/InternetTradersOfChildPornography.

5 The database is available at http://www.texaspredators.com/SexOffendersByCrime.aspx, accessed 9 November 2016.

6 Schulz, Anja et al. (2016), "Online Sexual Solicitation of Minors", 168.

7 Cortoni, Franca, Babchishin, Kelly M. and Rat, Cleménce (2016), "The proportion of sexual offenders who are female is higher than thought. A meta-analysis", *Criminal Justice and Behavior.* Published online before print July 15, 2016, doi: 10.1177/0093854816658923. Abstract available at http://cjb.sagepub.com/content/early/2016/07/15/0093854816658923.abstract, accessed 9 November 2016. This meta-analysis selected 17 sample studies from 12 countries, of which eleven were based on official records (i.e., arrests, charges, and/or convictions) and six on victimisation surveys. The study period considered covered data collected between 2000 and 2013.

8 Child Exploitation and Online Protection Center (2012), "Threat Assessment of Child Sexual Exploitation and Abuse 2012", London: CEOP, 11, accessed 9 November 2016, https://www.ceop.police.uk/Documents/ceopdocs/CEOPThreatA_2012_190612_web.pdf ; and Child Exploitation and Online Protection Center (2013), "Threat Assessment", 9.

9 Meter Onlus (2015), "Meter Report 2014: bambini 0-3 anni sempre più coinvolti, un orrore senza fine crimini contro l'infanzia", 5 March 2015, accessed 9 November 2016, http://www.associazionemeter.org/index.php/ct-menu-item-69/895-meter-report-2014-bambini-0-3-anni-sempre-piu-coinvolti-un-orrore-senza-fine-crimini-contro-l-infanzia.

10 Morris, Emma (2015), "#WePROTECT: Global Online Child Sexual Abuse Summit", Policy Brief, accessed 9 November 2016, https://www.fosi.org/policy-research/weprotect-global-online-child-sexual-abuse-summit/.

GENDER STEREOTYPING AND IMPACT OF FEMALE INTERNET SEX OFFENDING ON CHILD VICTIMS

In comparison to men, women are undoubtedly involved in Internet sex offending to a very limited extent. However, the significant proportion of identifiable females in victimisation surveys and self-report studies suggests that this offender population may likely be involved in these crimes to a higher degree than commonly perceived. As noted by Martellozzo et al. (2010), this wrong perception may be due to the fact that the discourse around online child sexual abuse and exploitation by women is largely influenced by gender constructs and stereotyping.

Even among professionals, there is a tendency to view women as victims rather than perpetrators, particularly of child sex crimes. Images of females sexually abusing children are therefore seen as particularly disturbing because they go against a common gender stereotype portraying women as either nurturing and protective mothers, or caregivers unable to sexually harm.[11] To rationalise the discomfort resulting from viewing these materials, the illegal acts committed by women are often justified by saying that online female sex offenders are 'sick' or have been coerced by a male.[12] When represented by the media, female Internet sex offenders are often demonised and described as 'inhuman'.[13]

How professionals in Spain reacted to the first case of child sexual abuse material possession and distribution involving a woman

In 2011, the Spanish police smashed a child sexual abuse material ring involving 10 people, including the first woman arrested for possession and distribution of child abuse materials in Spain.[14] According to news media, when police searched her home, they thought she was 'covering' for a man (a husband or a son) and were surprised to find that she had committed the crime alone.[15] In addition, a forensic psychiatrist interviewed about this case stated, "It is rare to see women abusing children because the maternal instinct prevents it. If women commit these crimes, it is because they are seriously sick".[16]

Gender stereotypes also fuel the notion that online female sex offending is less damaging than male sex offending and this may in turn affect victims' reporting. Sometimes children who disclose the abuse may not be believed by professionals, especially when the perpetrator is the victim's mother, and their sexual exploitation may be downplayed or treated as unimportant. Consequently, victims feeling isolated and stigmatised are discouraged from reporting.[17]

11 Martellozzo, Elena, Nehring, Daniel and Taylor, Helen (2010), "Online child sexual abuse by female offenders: An Exploratory study", *International Journal of Cyber Criminology* 4, n. 1 & 2 (2010): 600.

12 *Ibid.*

13 See also Bexson, Laura (2011), "The ultimate betrayal – Female child sex offenders", *Internet journal of Criminology*, accessed on 15 November 2016, http://www.internetjournalofcriminology.com/Bexson_Female_Child_Sex_Offenders_IJC_July_2011.pdf.

14 López-Fonseca, Óscar (2011), "Detenida por primera vez una mujer acusada de pedofilia", *Publico*, 1 March 2011, accessed 15 November 2016, http://www.publico.es/espana/detenida-primera-vez-mujer-acusada.html

15 Moya, Angel (2011), "La pedófila que quería adoptar un niño", *Telecinco,* 7 April 2011, accessed 15 November 2016, http://www.telecinco.es/informativos/sociedad/pedofila-queria-adoptar-nino_0_1200675158.html.

16 Rodríguez, Paco (2011), "La Policía «caza» a la primera mujer pedófila española que actuaba en internet", *La Razon,* 4 March 2011, accessed 16 November 2016, http://www.larazon.es/historico/4569-una-quiosquera-y-un-inspector-de-hacienda-detenidos-por-pornografia-infantil-TLLA_RAZON_361522?sky=Sky-Noviembre-2016#Ttt10017ntRjL4s0.

17 Cortoni, Babchishin and Rat (2016), "The proportion of sexual offenders", 2.

In the particular case of exploited boys, the commonly held belief that women are sexually passive while men are dominant and seeking sex with females pushes male victims to keep the abuse secret, or may result in failure to identify what happened to them as a violation of their rights. When boys do disclose, they may be viewed as 'weak' or be labelled as homosexual and, as a result, they may feel deeply ashamed.[18]

Moreover, female child sex offenders may take advantage of these stereotypical conceptions to carry on online child sexual abuse and exploitation without fear of detection or punishment. Not surprisingly, in the first study looking specifically at female Internet sex offending, Lambert and O'Halloran (2008) highlighted that recognition barriers play a key role in the perpetuation of these crimes by allowing women to have greater leeway in their access to and interactions with children.[19]

Despite prevalent misconceptions about the lack of harm women cause, the literature demonstrates that female child sex offending is as damaging as male offending. Immediate and long-lasting impacts on children appear to be similar to those of male-perpetrated abuse (e.g. depression, anxiety, suicidal thoughts, etc.); all the while presenting some variance and specificity (e.g. boys' confusion on sexual orientation and difficulty in trusting women in later life).[20] There is no research on the consequences of child sex crimes by females when they are committed online. However, studies of online sexual exploitation indicate that victims experience some of the effects of traditional sexual abuse victims (such as post-traumatic stress disorders), but at the same time, they display other specific types of mental health problems(such as they are more likely to experience running away from home, acting out sexually, and sexual victimisation).[21] The recovery of children abused and exploited by women in cyberspace must therefore address their special support needs as being both victims of female offending and individuals suffering child sex crimes in the online environment.

SOCIO-DEMOGRAPHIC CHARACTERISTICS

While studies have been conducted in recent years to understand the backgrounds of male Internet sex offenders,[22] there is a knowledge gap about the socio-demographic characteristics of females engaging in online sexual abuse and exploitation. The only investigation that explicitly examined this aspect identified through this review is a study into female consumers of child abuse materials published in 2010. By using self-reporting via an online survey, this study identified 10 women who were classified as consumers of child sexual abuse material; of these, the majority were aged between 18 to 35 years, completed higher education and were single.[23]

Although the sample analysed was small and not representative, these results seem to suggest that child sexual abuse material female offenders present similarities and differences from their male counterparts in terms of socio-demographic characteristics. A 2006 research on child sexual abuse material possessors in North America, for instance, found that male offenders were typically 40 years or older, single and well educated.[24]

The hypothesis that female perpetrators appear to be younger than men needs to be validated by

18 Mathews, Frederick (1997), "The Invisible Boy: Revisioning the Victimization of Male Children and Teens", Ottawa: National Clearinghouse on Family Violence, 35.

19 Lambert, Sharon and O'Halloran, Elaine (2008), "Deductive thematic analysis of a female paedophilia website", *Psychiatry, Psychology and Law* 15, n. 2 (2008): 286 and 299.

20 Stathopoulos, Mary (2014), "Female sex offending and the gendered nature of sexual violence", Melbourne: Australian Institute of Family Studies, 16-17, accessed 14 November 2016, https://aifs.gov.au/sites/default/files/publication-documents/ressum5.pdf.

21 Wells, Melissa & Mitchell, Kimberly J. (2007), ''Youth Sexual Exploitation on the Internet: DSM-IV Diagnoses and Gender Differences in Co-occurring Mental Health Issues'', *Child and Adolescent Social Work Journal* 24 (2007): 256-257.

22 See, for example, Reijnen, Lotte, Bulten, Erik and Nijman, Henk (2009), "Demographic and Personality Characteristics of Internet Child Pornography Downloaders in Comparison to Other Offenders", *Journal of Child Sexual Abuse* 18 (2009): 611–622.

23 Seigfried-Spellar Katherine C. and Rogers Marcus (2010), "Low neuroticism and high hedonistic traits for female internet child pornography consumers", *Cyberpsychology, Behavior and Social Networking* 13, n. 6 (2010): 632.

24 Wolak, Janis, Mitchell, Kimberly and Finkelhor, David (2011), "Child Pornography Possessors: Trends in Offender and Case Characteristics", *Sexual Abuse: A Journal of Research and Treatment* 23, n. 1 (2011): 29.

further research because current knowledge is too limited for drawing reliable conclusions. For example, an analysis of a sample of 14 women included in a public database of registered sex offenders in Texas seems to contradict this finding,[25] indicating that the majority of female perpetrators convicted for possession of child sexual abuse materials in the state were slightly older (seven were aged 40 years or older).[26]

On the other hand, a 2005 survey concerning online victimisation of youth in the US points to young female sex offenders, revealing that 64% of the females who made aggressive sexual solicitations online were younger than 18, and 36% were 18 to 24.[27] Taken together, these results show that women engaging in online child sexual abuse and exploitation may be both young and old, adults and juveniles, and that their age will likely vary according to the type of ICT-facilitated offence they commit.

No research has investigated the employment occupations of online female child sex offenders. However, a review of 51 cases of British women who engaged in online exploitation included in a public database of sex offenders managed by an Internet watchdog[28] provides preliminary insights into this characteristic. Of the 23 cases for which information on employment is available, analysis of the sample shows that a consistent number of female offenders had an employment involving direct contact with children (e.g. teachers, helpers in nursery schools, baby sitters, etc.).

From this point of view, there appears to be no substantial difference between women involved in Internet sex offending and those engaging in contact offences. As literature demonstrates, "most sexual abuse by females takes place in the care giving environment, often in the context of their role as nurturer, in the family home, nurseries, schools and community settings".[29] Female sex offenders also appear to be employed in child-centred professions more frequently than men.

In fact, of the 23 cases in the British sample, 78% of female dual offenders (i.e. those that committed both contact and non-contact offences) and 55% of those who engaged only in online sexual abuse and exploitation were found to be working with children and adolescents.[30]

This proportion seems to be lower in the case of men. According to the abovementioned research on male child sexual abuse material possessors in North America, 20% of dual offenders and 11% of online sexual abuse and exploitation only offenders accessed children through their employment.[31] Rather than reflecting a difference in their offending behaviours, this possible trend should be seen as the result of a general higher prevalence of female employment in professions involving contact with children.

25 The 14 cases analysed are available at:
1) http://www.texaspredators.com/SexOffender.aspx?oid=20242;
2) http://www.texaspredators.com/SexOffender.aspx?oid=9166 ;
3) http://www.texaspredators.com/SexOffender.aspx?oid=56132 ;
4) http://www.texaspredators.com/SexOffender.aspx?oid=17489 ;
5) http://www.texaspredators.com/SexOffender.aspx?oid=18176 ;
6) http://www.texaspredators.com/SexOffender.aspx?oid=18269 ;
7) http://www.texaspredators.com/SexOffender.aspx?oid=22878 ;
8) http://www.texaspredators.com/SexOffender.aspx?oid=21634;
9) http://www.texaspredators.com/SexOffender.aspx?oid=53095 ;
10) http://www.texaspredators.com/SexOffender.aspx?oid=453;
11) http://www.texaspredators.com/SexOffender.aspx?oid=11660 ;
12) http://www.texaspredators.com/SexOffender.aspx?oid=16463 ;
13) http://www.texaspredators.com/SexOffender.aspx?oid=31977;
14) http://www.texaspredators.com/SexOffender.aspx?oid=31143 .

26 With regard to race, only 3 out of 14 offenders were Hispanic. In terms of age, 7 offenders were 40 years or older, 1 between 18 and 25, and 6 between 26 and 39.

27 Wolak, M. and Finkelhor (2006), "Online Victimization of Youth", 17.

28 The database of female sex offenders is available at: https://theukdatabase.com/category/female-abuser/ Offered by a legal Internet watchdog, this is the only public database of convicted child abusers, paedophiles and child killers for the UK and Ireland. It also contains information on support for survivors and safety tips. The cases selected and analysed in this article include women that have been arrested for different ICT-facilitated child sex crimes. The type of offences for which they have been convicted include among others: meeting a child following sexual grooming with the intent of abusing them; making, viewing or distributing child abuse images; allowing someone else to make, view or distribute child abuse images; showing pornography to a child and inciting a child to take part in sexual activity online.

WHAT TYPES OF CRIME DO FEMALE CHILD SEX OFFENDERS CARRY OUT ONLINE?

While bringing many benefits to society, fast-paced technological innovation and increasing accessibility of ICTs also provide new pathways to the sexual abuse and exploitation of children. Similar to male offenders, females may take advantage of the sense of anonymity, impunity, disinhibition and depersonalisation afforded by the Internet to explore the darker side of sexuality and engage in deviant sexual behaviours.

Literature and empirical evidence indicate that some women misuse online technologies for the commission of a wide variety of traditional and emerging child sex offences. The first research into female Internet sex offenders provides insight into a paedophilia website created and accessed by women, concluding that this population displays similar characteristics to male individuals when offending online.[32]

Besides accessing paedophilia websites, females have been found to engage in possession, production, trading and distribution of child sexual abuse materials (CSAMs). Using an online survey, research by Seigfried et al. (2008) attempted to determine the prevalence rate of CSAM consumption, revealing that females engaged in these unlawful acts more often than previously thought, particularly given that 5.5% of the sample self-reported as female CSAM consumers.[33]

An exploratory analysis to deepen understanding of female possessors of child sexual abuse material.

An exploratory analysis of the abovementioned public database of sex offenders in the UK offers initial hints about female possessors of CSAM. The database includes several cases (17 in total) of British women convicted for possession and downloading of CSAM requiring further scrutiny. Based on information available, it appears that a majority of the female offenders arrested, possessed a limited number of child sexual abuse images (less than 30). Pictures were often in the most serious category (i.e. involving penetrative sexual activity or sexual activity with an animal or sadism) and depicted predominately prepubescent children. Notably, over one third of the females found in possession of CSAM were dual offenders (i.e. women who also committed contact child sex offences or grooming) and, in three cases, there was a clear crime escalation from possessing, viewing and downloading CSAM to committing (or trying to commit) contact child sexual abuse. Although these preliminary findings are not representative, nor are the result of scientific research, they do suggest that female possessors of CSAM might share some commonalities with male offenders. The abovementioned research on CSAM possessors in North America found that the largest proportion of males had images depicting mostly girls and prepubescent children, and showing penetration of a child and sexual contact between children and adults. Of all arrested CSAM possessors, 41% were dual offenders, a proportion very similar to that of female offenders in the British sample.[34] On the other hand, males appeared to collect higher numbers of child abusive images compared to women (about half of the male offenders possessed more than 100 graphic still images).[35] These preliminary results should by no means be considered generalisable because the proportion of male dual offenders possessing CSAM varies consistently across available research, ranging from 5 to 85%.[36]

29 Reconstruct, "What is known about female sex offenders and the impact on their victims?", accessed 16 November 2016, http://www.reconstruct.co.uk/public/docs/news/Female_sex_offenders.pdf.

30 The database of female sex offenders is available at: https://theukdatabase.com/category/female-abuser/.

31 Wolak, Mitchell and Finkelhor (2011), "Child Pornography Possessors", 35.

32 Lambert and O'Halloran (2008), "Deductive thematic analysis of a female paedophilia website", 298.

33 Seigfried, Lovely and Rogers (2008), "Self-reported online child pornography behavior".

34 Wolak, Mitchell and Finkelhor, David (2011), "Child Pornography Possessors", 30 and 33.

35 *Ibid.*, 7.

36 This observation was made by the peer-reviewer of this article.

A proportion of female Internet sex offenders fuel the market in child sexual abuse and exploitation by trading, collecting and exchanging CSAMs. Analysing the media coverage of convicted and sentenced Internet offenders from 1996 to 2002, a study by Alexy et al. identified 133 cases of 'traders' or collectors of CSAMs, of which 5.3% involved females.[37] As noted with males, women may actively seek, collect or share CSAM using peer-to-peer networks (such as Gnutella)[38] or through the 'Dark web' which makes tracking and counteraction of these illegal practices more difficult and hidden.[39] The exchange of CSAM may be a condition for acceptance in online paedophile communities[40] and may occur for commercial purposes; especially when the images are produced and circulated with the deliberate intent to get compensation.[41]

Despite the fact that data on prevalence rates for female involvement in CSAM production are unavailable, there is abundant evidence that women contribute to this offence to a quite significant extent and in a variety of ways. CEOP's 2013 "Threat Assessment of Child Sexual Exploitation and Abuse" found that 24% of the images of child abuse analysed between January 2010 and December 2012, depicted sexual contact between a child and an adult female.[42] Women may record their own abuse or that of others, or may induce children to submit images of themselves (i.e. self-generated sexually explicit content). Sometimes females engage in the making of CSAM by committing contact sexual abuse of children that is recorded by others (e.g. male partners).

Moreover, with the rapid evolution in ICTs and the emergence of new devices and tools on the market, an issue of concern requiring further investigation is the active participation of women in ordering and live streaming child sexual abuse. While evidence of female perpetrators implicated as 'end-users' or 'consumers' of this new form of online child sexual abuse and exploitation is lacking, incidents of women forcing children to perform sex acts online, or live streaming their own child sexual abuse, are emerging primarily in South-East Asia (particularly the Philippines),[43] and more recently in some Western countries (e.g. USA[44] and UK[45]).

An equally disturbing trend is the significant involvement of females in the online solicitation or grooming of children for sexual purposes. A 2010 survey regarding online victimisation of youth in the USA found that 16% of those carrying out aggressive sexual solicitation of children online were female.[46] Additional research targeting adult Internet users in Germany, Sweden and Finland confirms that the proportion of female perpetrators engaging in online sexual solicitation is substantial, ranging from 17.2% for solicitation of children to 30.6% for solicitation of adolescents.[47]

37 Alexy, Eileen M., Burgess, Anna W. and Baker, Thomas (2005), "Internet offenders", 804-12.

38 See, for example, the case mentioned in López-Fonseca, Óscar, "Detenida por primera vez una mujer acusada de pedofilia", Publico, 1 March 2011, accessed 15 November 2016, http://www.publico.es/espana/detenida-primera-vez-mujer-acusada.html.

39 See the case of a female paedophile sharing CSAM cited in Knox, P., "Revealed -The deep web: Where paedophiles like UK's worst Richard Huckle do as they please", *Dailystar,* 6 June 2016, accessed 15 November 2016, http://www.dailystar.co.uk/news/latest-news/521079/dark-deep-web-tor-richard-huckle-hidden-paeophile-world.

40 "Kate Seekings – Havant", https://theukdatabase.com/2012/06/17/kate-seekings-havant/.

41 See, for example, the recent case of a Colombian woman who sold to an American paedophile network videos of child sexual abuse with her two children: "Detienen mujer colombiana por grabar pornografia infantil con sus hijos", accessed 15 November 2016, http://www.ahoranoticias.cl/noticias/mundo/detienen-a-mujer-colombiana-por-grabar-pornografia-infantil-con-sus-hijos.html.

42 Child Exploitation and Online Protection Center (2013), "Threat Assessment of Child Sexual Exploitation", 9.

43 UROPOL- European Cybercrime Centre (EC3) (2013), "Commercial Sexual Exploitation of Children Online: A Strategic Assessment", 8, https://www.europol.europa.eu/publications-documents/commercial-sexual-exploitation-of-children-online.

44 Seales, Rebecca (2012), "Mother jailed after making 10-year-old daughter pose nude on Skype to enter fake $20,000 mom-child bikini shoot contest", *Daily Mail*, 1 March 2012, accessed 15 November 2016, http://www.dailymail.co.uk/news/article-2108565/Mother-jailed-making-10-year-old-daughter-pose-nude-Skype-enter-fake-20-000-mom-child-bikini-shoot-contest.html#ixzz4RIbyXQMA.

45 Robertson, Alexander, "Schoolgirl, 13, was abused by 137 paedophiles including a teacher after her profile was posted on a swingers website without her knowledge", *Daily Mail*, 12 August 2016, accessed 15 November 2016, http://www.dailymail.co.uk/news/article-3735760/Schoolgirl-13-abused-137-paedophiles-including-teacher-profile-posted-swingers-website-without-knowledge.html#ixzz4RIaKBvYy.

46 Wolak, Janis *et al.* (2014), "Trends in Unwanted Online Experiences and Sexting: Final Report. 2014".

47 Schulz, Anja *et al.* (2016), "Online Sexual Solicitation of Minors", 177.

Another abusive act linked to online sexual solicitation of children in which female perpetrators may engage is sexual extortion. Although little is known about this new type of offence, there is an emerging indication that some women befriend adolescents online and later blackmail them with the help of self-generated images of the victims in order to extort sexual favours, money, or other benefits from them under the threat of sharing the material with others.[48]

There have also been cases of adult women or young adolescents who, in the wake of face-to-face romantic or sexual relationships during which sexual images were taken or shared, have threatened to disseminate images of their ex partners aged under 18 either in order to force reconciliation or to embarrass or humiliate them online (so called 'revenge porn'). A recent survey on sexual extortion involving over 1,600 victims found that perpetrators in face-to-face relationships were female in 9% of cases, with almost half of the victims being younger than 18 when the incidents began.[49]

TYPOLOGIES OF INTERNET FEMALE SEX OFFENDERS AND OFFENDING MOTIVATIONS

To support greater detection and more effective management and treatment of female sex offenders, researchers developed typologies describing offender criminogenic characteristics, victim profiles, offender modus operandi and motivations for offending.[50] However, efforts of this kind focus primarily on women committing contact child sex crimes while attention to female Internet perpetrators remains scant. The study on women using a paedophilia website by Halloran and Lambert (2008) is an exception to this.

Based on a thematic analysis, this research examines some of the motivations behind female online child sex offending, while also highlighting the supporting role that cognitive distortions, recognition barriers and the Internet itself play in perpetuating these illegal practices. Questioning the validity of those theories of abusive women that do not acknowledge female deviant sexual interest, these authors have found that females contributing to paedophilic forums exhibit a clear sexual attraction to children and a strong desire for sexual contact with them.[51] This suggests, similar to male perpetrators, some women carrying out ICT-facilitated sex offences against children may be affected by paedophilia (i.e. a sexual disorder involving an intense and recurrent sexual interest in prepubescent children); or that the women may display an atypical sexual preference to pubescent children (otherwise known as 'hebephilia').

In addition to sexual motivation, Lambert and O'Halloran (2008) also note an association between female illicit sexual behaviours online and some traits in their personality. More specifically, female users of the pro-paedophilia website appeared to show dissatisfaction with current persona, as well as problems resulting from early sexualised experiences and poor adolescent socialisation. These personal factors had already been identified in previous research on problematic use of the Internet by male offenders and were found to make an individual more prone to engaging in the inappropriate use of technology.[52]

Based on some of the criminogenic areas highlighted by Lambert and O'Halloran, Elliott and Ashfield (2011) conducted another in-depth analysis of the modus operandi of female Internet sex offenders. Drawing from clinical cases, the study sought to grasp the characteristics of this population using the literature on female sexually offending offline

48 See, for example, Othmann, Hannah, "Police investigation launched after teenager is blackmailed by woman he met online", *Evening Standard,* 2 February 2016, accessed 15 November 2016, http://www.standard.co.uk/news/crime/police-investigation-launched-after-teenager-is-blackmailed-by-woman-he-met-online-a3171461.html; and "L'Aquila: ricatto hard a minore, 200 Euro o metto foto in rete", 19 September 2016, accessed 15 November 2016, http://www.abruzzoweb.it/contenuti/l-aquila-ricatto-hard-a-minorenne-dammi-200-euro-o-metto-foto-in-rete-/610022-4/.

49 Wolak, Janis and Finkelhor, David (2016), "Sextortion: findings from a survey of 1,631 victims", 71, accessed 15 November 2016, https://www.wearethorn.org/sextortion/.

50 Stathopoulos, Mary (2014), "The exception that proves the rule", 10-12.

51 Lambert, Sharon and O'Halloran, Elaine (2008), "Deductive thematic analysis", 289-290.

52 *Ibid*., 295 and 299.

as a reference point. Echoing Lambert and O'Halloran, an important criminogenic factor pinpointed by these authors are interpersonal and socialisation deficits.

In the authors' view, many women engaging in Internet sex crimes have difficulties maintaining healthy relationships, especially after experiencing childhood abuse. Very often, female perpetrators consider romantic and sexual relationships as the only source of their self-worth and, in the absence of a satisfying intimate life, may resort to online technology to initiate virtual liaisons (for example through dating websites), which are perceived as safer than face-to-face contacts.[53]

Using existing typologies, Elliott and Ashfield identified two subgroups of online FSOs displaying interpersonal and socialisation deficits: (1) solo offenders against adolescents and (2) male-associated offenders. The first category, also known as the teacher lover/ heterosexual nurturer, includes females sexually abusing or exploiting young teenage boys (usually aged 12-13 years old) often in the context of a position of authority or trust (a family member or friend, a teacher, etc.).[54]

Self-initiated online abusers (such as online solicitors) do not see their behaviour as abusive and appear to exhibit emotional loneliness, often resulting from a dysfunctional adult relationship. They usually fall in love with their victims or believe they are teaching them about sexuality. By developing bonds with male adolescents, these women seek to fulfil their intimacy and sexual needs while also experiencing the feelings of power and control typically lacking with adult partners.

Despite being based on clinical work, Elliott and Ashfield warn that this interpretation of female online solo offending may reproduce a gender bias where women engaging in online sexual abuse and exploitation are assumed to be pushed by a need for intimacy, whereas men are motivated by sexual gratification. This distinction may be inappropriate and its validity should be individually assessed during treatment.[55]

It must also be recalled that besides solo offenders victimising adolescent males, women offending alone may target prepubescent children or pubescent females, in which case the motivations may be different. For those sexually molesting younger children (also known as predisposed offenders), literature indicates that they are often prompted to offend for sexual arousal or by the need to re-enact the physical and sexual abuse they suffered from their caregivers during childhood.[56]

For those exploiting young pubescent females, research has found that offenders can be motivated, among others, by financial gain.[57] As far as online child sexual exploitation is concerned, an example could be that of women forcing their daughters to engage in live streaming or in prostitution and subsequent production of CSAMs in exchange for compensation.[58] With different motivations, another scenario could be that of same-sex online grooming by homosexual women posing as young boys or girls in order to draw female adolescents into online and/or offline sexual activities.[59]

The second sub-group described by Elliott and Ashfield are male-associated offenders committing online child sex crimes with another, typically male, adult. In addition to displaying intimacy deficits, these female perpetrators have been described as emotionally dependent, passive and possessing low self-esteem. Some women are coerced into online sexual offending

53 Elliott, Ian A. and Ashfield, Sherry (2011), "The use of online technology the modus operandi of female sex offenders", *Journal of Sexual Aggression* 17, n. 1, 3-4.

54 *Ibid.*, 5.

55 *Ibid.*, 5-6.

56 Simons, Dominique A. (2014), "Chapter 3: Sex Offender Typologies", in *Sex offender management, assessment and planning initiative,* eds. Holder, Eric H. Jr., Mason, Karol V. & de Baca, Luis C., Washington: U.S. Department of Justice - Office of Justice Programs, 60.

57 *Ibid.*

58 See, for example, Filetto, Giuseppe, "Baby squillo della Genova-Bene "Processate i clienti", *La Repubblica,* 8 May 2016, accessed 5 December 2016, http://ricerca.repubblica.it/repubblica/archivio/repubblica/2016/05/08/baby-squillo-della-genova-bene-processate-i-clienti Genova07.html?ref=search.

59 See, for example, the case of "Natalie Reed – Dagenham" reported by the media in the UK in June 2011 and included in the "UK database of sex offenders", accessed 5 December 2016, https://theukdatabase.com/2012/04/15/natalie-reed-dagenham/.

by an accomplice and may be motivated by fear of violence.[60] Martellozzo et al. (2010) stresses that coercion is frequently mentioned as a push factor in cases of female Internet sex offenders, but ascertaining that force was used against a woman is difficult, especially from the sole analysis of CSAMs.

Moreover, female offenders, like all perpetrators, may be tempted to blame other people rather than taking responsibility for their actions. This behaviour is further reinforced by the fact that, in contrast to male offenders, females are usually not perceived as sexually aggressive and as such, their claim of having been coerced by a male accomplice is usually accepted 'without substantial proof', including by frontline professionals.[61] As expected, the great majority of Internet female perpetrators in the study by Martellozzo et al. denied their offending conduct and blamed their partners for compelling them into committing child sex crimes.[62]

As in Elliott and Ashfield's research, most of the women had a history of failed, poor and abusive relationships, and were highly dependent on their partners, thereby allowing easy manipulation into illegal sexual acts against children. Many female offenders took pictures of abuse of their own children to please their (often only virtual) 'lovers' and maintain their attention, without perceiving the real harm suffered by their victims.[63]

Besides coercion or manipulation by a male, some female co-perpetrators actively participate in the offending process by directly engaging in hands-on abuse. Conversely, others play a more passive role by not taking proper measures to prevent victimisation or procuring victims for their male partners.[64] Female perpetrators offending with a male and taking an active role have been found to be motivated by anger and jealousy, and reportedly, often act to fulfil a need for revenge.[65] 'Passive' female offenders, like those being coerced by a male, may facilitate the abuse for fear of losing their partner, inability to protest or lack of autonomy and self-reliance.

While typologies assist professionals in appreciating the crime, it must be recalled that female Internet sex offenders are a heterogeneous group "that cannot be accurately characterised with one-dimensional labels".[66] The relationships between offender, offence and victims are often unique and diverse, making categorisation difficult and incongruous. Also, as Martellozzo et al. point out, the utility of classifying people into distinct typologies with rigid boundaries should be questioned because this may contribute to reproducing and reinforcing gender stereotypes.[67]

EXPLORING DIFFERENCES BETWEEN MALE AND FEMALE INTERNET SEX OFFENDERS

When examining cyber-enabled child sexual abuse and exploitation by females, an issue deserving more in-depth investigation is whether the differences between males and females identified in research regarding hands-on abuse

60 Elliott, Ian A. and Ashfield, Sherry (2011), "The use of online technology", 5.

61 Martellozzo, E., Nehring, D. and Taylor, H. (2010), "Online child sexual abuse by female offenders", 602.

62 *Ibid.,* 603.

63 *Ibid.,* 604-605.

64 Grayston, Alana D., and De Luca, Rayleen V. (1999), "Female perpetrators of child sexual abuse: A review of the clinical and empirical literature", *Aggression and Violent Behavior* 4, n.1 (1999): 96. Examples of women that can be defined as "passive male-accompanied" Internet sex offenders include: a) "Violenta una bambina scopre che è la figlia", *La Repubblica,* 18 November 2011, accessed 5 December 2016, http://ricerca.repubblica.it/repubblica/archivio/repubblica/2011/11/18/violenta-una-bambina-scopre-che-la-figlia.html?ref=search; 2) the case of a mother who refused to believe that her daughter was abused by her father, even when the girl showed her a picture of the abuse. Cit. in Adams, Christine (1994), "Mothers Who Fail to Protect Their Children from Sexual Abuse: Addressing the Problem of Denial", Yale Law & Policy Review 12, n. 2 (1994): 522.

65 Nathan, Pamela and Ward, Tony (2002), "Female sex offenders: Clinical and demographic features", *Journal of Sexual Aggression* 8, n. 1 (2002): 5–21. For active male-accompanied online female offenders, see, the case of "Peter/Suzie Phillips – Newport" reported in 2012-2013 by the media in the UK, accessed on 5 December 2016, https://theukdatabase.com/2012/08/14/petersuzie-phillips-newport/.

66 Martellozzo, E., Nehring, D. and Taylor, H. (2010), "Online child sexual abuse by female offenders", 594.

67 *Ibid.*

are applicable to cases of female Internet sex offenders. A 2014 literature review by Simons (2014) highlights three key differences between male and female perpetrators:

a) In contrast to male sexual offenders, female offenders are more likely to sexually assault males and strangers […];

b) Female sexual offenders are less likely than male sexual offenders to sexually reoffend […]; and

c) Female offenders are more likely to sexually assault with another person or group.[68]

The fact that women primarily target males and strangers is widely disputed. In particular, recent studies highlight that females are less discriminating than males with regards to victims' gender. Moreover, it is claimed that they are more likely than male perpetrators to abuse or exploit their biological children, or children in their care.[69] Given that many women offending through ICTs have been found to victimise their own children or children under their supervision, the latter observation appears to be pertinent when examining the occurrence of online female-perpetrated child sexual abuse and exploitation.

As for victims' gender, literature and available evidence do not provide conclusive results. For example, a recently published study concerning online solicitation of minors found that female perpetrators were more likely to contact male children and adolescents as compared to men (71.1% versus 45.5%), and found an equal distribution of contact with female victims among male (67.7%) and female offenders (60.5%).[70] On the other hand, the review of an Australian NGO database of sex offenders reveals that 6 out of 8 victims of female Internet sex offending were girls (involving mainly production, distribution and possession of CSAMs).[71]

Previous offence history and recidivism rate of females engaging in online child sexual abuse and exploitation have not been specifically studied. However, there is some indication that women perpetrating this type of crime rarely have past convictions for child sex crimes. Research by Beech et al. (2009) found that 1 of 4 women convicted for ICT-facilitated offences included in their study was previously sentenced for non-sexual crimes.[72]

Similarly, based on publicly available information, the analysis of the NGO database of sex offenders in the UK suggests that none of the 51 female offenders had a prior conviction for sexual crimes, whereas one had a conviction of a non-sexual offence,[73] and another received a reprimand for sexual assault against a child.[74] For women co-offending with a male accomplice, the analysis also shows that men are more likely to serve sentences for sex offences than their female counterparts. Of all males implicated in the cases examined, 5 had prior convictions for sex crimes, including against children,[75] and one received a police caution for possession of CSAMs.[76] This finding appears to corroborate

68 Simons, Dominique A. (2014), "Chapter 3: Sex Offender Typologies", 59.

69 Williams, Katria S. and Bierie, David M. (2014), "An Incident-Based Comparison of Female and Male Sexual Offenders", *Sexual Abuse: A Journal of Research and Treatment,* published online on 29 July 2014, DOI: 10.1177/1079063214544333, 3.

70 Schulz, Anja *et al*. (2016), "Online Sexual Solicitation of Minors", 177-178.

71 These cases are included in the database managed by the Australian NGO Mako. See "MAKO/Files Online - Listing Australian Paedophiles/ Sex Offenders/ Child Killers", accessed 6 December 2016, http://www.mako.org.au/temp_female.html.

72 Beech, Anthony *et al.* (2009), "Assessing female sexual offenders' motivations and cognitions: an exploratory study", *Psychology, Crime & Law* 15, n. 2-3 (2009): 205.

73 "Colin Blanchard Paedophile ring", accessed 6 December 2016, https://theukdatabase.com/2012/03/09/colin-blanchard/; and "Nursery sex abuse case: Profiles of Vanessa George, Colin Blanchard and Angela Allen", The Guardian, 1 October 2009, accessed 6 December 2016, https://www.theguardian.com/society/2009/oct/01/nursery-sex-case-abusers-profiles

74 "Sadie Morris – Barwell", accessed 6 December 2016, https://theukdatabase.com/2016/07/21/sadie-morris-barwell/.

75 See "Jane Voss", accessed 6 December 2016, https://theukdatabase.com/2012/03/09/jane-voss-wanstead/; "Neil Bowyer/Susan avison", accessed 6 December 2016, https://theukdatabase.com/2012/06/15/neil-bowyersusan-davison-washington/ ; "Marie Raison – Dagenham", accessed 6 December 2016, https://theukdatabase.com/2013/12/13/marie-raison-dagenham/; "Stephen/Amanda Wholey – Glapwell", accessed 6 December 2016, https://theukdatabase.com/2013/09/19/stephenamanda-wholey-glapwell/; "Joanne Gibson – Broadstairs", accessed 6 December 2016, https://theukdatabase.com/2013/05/08/joanne-gibson-broadstairs/.

the conclusion that some known male offenders may use the Internet to contact women with the explicit intent of persuading them into participating in online sexual abuse and exploitation.

Limited information is available on whether female Internet sex offending is more likely to involve a direct male accomplice. Research by Martellozzo et al. found that the majority of females in their study offended with their partners.[77] The review of the NGO database of sex offenders in the UK reveals similar results. Of the 51 cases of female perpetrators convicted for online sexual abuse and exploitation, 31 involved a male co-offender (e.g. husband, secret lover met online, partner, colleague, friend, etc.). Compared to male Internet offenders, women engaging in cyber-enabled child sex offences are less likely to offend alone or to participate in criminal networks. According to Interpol, only 1 percent, at the most, of those involved in CSAM rings are female.[78]

As for prevalence rates of male co-offending, a 2006 research on CSAM possessors in North America, found that only in 5% of cases analysed, perpetrators (virtually all males) offended with an accomplice.[79] Females abusing children through ICTs also appear less likely to offend alone when compared to females engaging in contact sexual offences. A recently released study by Budd et al. (2015) suggests that the majority of women in their sample were solo offenders (62%); and approximately 24% committed a sex crime with a male while 6% offended with one or more females.[80]

CONCLUSION AND RECOMMENDATIONS

Though in its nascent state, academic literature supported by evidence from all world regions highlights the significance of examining the issue of female Internet sex offending in its multiple forms. Contrary to a common misconception that downplays or neglects the involvement of women in relevant online activities, it is now irrefutable that some females do commit ICT-facilitated child sex crimes and play different roles in the offending process. As stressed by Martellozzo et al., current knowledge indicates, "women may actively participate in the online abuse of children, they may coerce or coax children into submitting to acts of abuse, and they may play a significant role in facilitating abuse by male offenders."[81]

By examining their multi-faceted function and diverse motivations, this article suggests that while female Internet sex offenders share many characteristics with women abusing children offline, they may also present some particular traits (e.g. younger age, likely higher prevalence of co-offending particularly among dual offenders). At the same time, it would appear that women involved in cyber-enabled child sexual abuse and exploitation are a comparatively distinct group of perpetrators overlapping partially with male Internet sex offenders. Like their male counterparts, women acting online are not a homogenous group. They may display similar behaviours and thinking styles to men,[82] and be driven by a range of criminogenic factors (e.g. sexual arousal/motivation, use of cognitive distortions, personal factors such as early sexualisation and dissatisfaction with current persona, socialisation and interpersonal deficits, etc.).

However, in comparison to males, female Internet sex offenders can often display a strong need for intimacy (though this may also be true for men) which may induce them to establish inappropriate relationships with children or, alternatively, leave them particularly vulnerable to manipulation and

76 "Colin Blanchard Paedophile ring", accessed 6 December 2016, https://theukdatabase.com/2012/03/09/colin-blanchard/

77 Martellozzo, E., Nehring, D. and Taylor, H. (2010), "Online child sexual abuse by female offenders", 603.

78 "23 women found guilty of child pornography", Radio Sweden, 18 October 2011, accessed 6 December 2016, http://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=4752927,

79 Wolak, Janis, Mitchell, Kimberly and Finkelhor, David (2011), "Child Pornography Possessors", 30.

80 Budd, Kristen M., Bierie, David M. and Williams, Katria (2015), "Deconstructing Incidents of Female Perpetrated Sex Crimes: Comparing Female Sexual Offender Groupings", *Sexual Abuse: A Journal of Research and Treatment*, published online before print July 10, 2015, DOI: 10.1177/1079063215594376, 6.

81 Martellozzo, E., Nehring, D. and Taylor, H. (2010), "Online child sexual abuse by female offenders".

82 Lambert and O'Halloran (2008), "Deductive thematic analysis of a female paedophilia website", 298.

coercion by predatory males, both online and offline. Typical characteristics of these women are low self-esteem, dependency, emotional loneliness, passivity and involvement in abusive relationships during adulthood.

In addition, research indicates that:

a) Women engaging in cyber-enabled child sex offences use a number of recognition barriers to cover and justify their abusive behaviours;

b) They are more likely than male perpetrators to abuse or exploit in care giving situations;

c) They are less likely to offend alone or to participate in criminal networks; and

d) They are less likely to have past convictions for sex offences and, possibly, they tend to re-offend to a lower extent compared to male perpetrators.

The peculiarity of female Internet child sex crimes has a number of implications for offenders' treatment as well as for policy and programme development. Stemming from different gender roles attributed to men and women since childhood, female (and male) norms require that a gender-responsive approach be adopted by all actors and sectors involved in addressing this problem (including law enforcement, treatment providers, caregivers and other frontline professionals, civil society, private sector, media, academia, etc.).

While strategies to date focus predominantly on male offenders, there is clearly a need to put females engaging in online child sexual abuse and exploitation on the radar. As this literature review suggests, research efforts should spearhead a deepened understanding of female Internet sex offenders, their socio-demographic characteristics and motivations, the profile of their victims, as well as the modalities through which they come to act as participants, instigators, and facilitators. The prevalence rate of female online sex offending should also be further investigated through quantitative research.

Moreover, while abundant research has explored the different psychological profiles and characteristics of males who are Internet offenders, contact offenders or dual offenders, there is a knowledge gap when it comes to women.[83] Data suggests that a high proportion of female perpetrators of child sex crimes on the Internet engage in hands-on abuse and this crossover deserves to be analysed and understood. Likewise, the prevalence of female recidivism, co-offending and the use of coercion by male partners, as well as the role played by CSMA in the development and escalation of deviant sexual interests in women are all areas requiring better understanding. Last but not least, research is needed to review what has been done to address the issue, identify good practices and programme gaps, and propose concrete recommendations for action.

In addition to more research, there is a need to ensure the adoption of adequate legislation, as well as effective and proactive detection, investigation and prosecution of female Internet sex offenders. Comprehensive laws are required to punish all illegal acts related to child sexual abuse materials (mere possession, production, distribution, viewing/accessing), including 'virtual child pornography'. Moreover, in light of the involvement of female (and male) offenders in new forms of Internet-related crimes, legislation should be introduced to criminalise online grooming (possibly extending protection from this crime to all children under 18 years, and not only up to the legal age of consent as happens in many States), live-streaming of child sexual abuse and sexual extortion.

It is essential that all these pieces of legislation use gender neutral language, protecting both girls and boys as victims and criminalising both male and female offenders. In terms of law enforcement, it is crucial to guarantee an adequate level of punishment of female Internet sex offenders. As many studies demonstrate, "women are likely to receive more lenient sentences than men as a patriarchal legal system looks to protect women, views women as less responsible for their criminal offenses, and views women as in need of help and protections".[84]

83 Elliot, Ian A. and Beech, Anthony (2009), "Psychological Profiles of Internet Sexual Offenders: Comparisons With Contact Sexual Offenders", *Sexual Abuse: A Journal of Research and Treatment* 21, n.1 (2009): 76-92; Elliot, Ian A. and Beech, Anthony (2013), "The Psychological Profiles of Internet, Contact, and Mixed Internet/Contact Sex Offenders", *Sexual Abuse: A Journal of Research and Treatment Sex Abuse February* 25, n. 1 (2013): 3-20; Babchishin, Kelly M., Hanson, R. Karl & Van Zuylen Heather (2015), "Online Child Pornography Offenders are Different: A Meta-analysis of the Characteristics of Online and Offline Sex Offenders Against Children", *Archives of Sexual Behavior* 44, n. 1 (2015): 45-66.

84 Marcum, Catherine D., Higgins, George E. and Richard Tewksbury (2011), "Doing Time for Cyber crime: An Examination of the Correlates of Sentence Length in the United States", *International Journal of Cyber Criminology* 5, n. 2 (2011): 828.

Research using data from the United States Sentencing Commission (covering the period 2001-2003) confirms that this is true for different types of crimes, including CSAM related offences.[85] In contrast to what criminal justice scholars defined as the "chivalry hypothesis of female offending", women should not be treated differently from male offenders when it comes to sentencing.

Better law enforcement and appropriate punishment should be part of a broader preventive strategy which tackles Internet child sex offending by females in a comprehensive and coordinated manner, with the participation of all relevant stakeholders. As increasingly recognised by the civil society community, one such strategy to address the demand for child sexual abuse and exploitation, including when ICTs are used to perpetrate it, is based on a public-health model involving three layers of intervention: primary, secondary and tertiary prevention.[86] As with male offenders, it is crucial that this multi-faceted combination of preventive interventions to be put in place to solve the issue of female Internet sex offending.

Primary prevention targets the general population (including all children and youth) and involves a number of interventions aimed at averting the problem before it would otherwise occur. Strategies of this kind may include:

1) Raising awareness of children, adolescents and different duty-bearers (police, legal actors, therapists, primary health care professionals, media, etc.) about female-perpetrated online child sexual abuse and exploitation, the impact of gender stereotyping and consequences for victims. In this framework, specific information campaigns should be undertaken to dispel myths including:
   a That only men commit child sex crimes on the Internet;
   b Women are nurturers so they cannot engage in cyber-enabled abuse and exploitation or, if they do so, their involvement is very rare;
   c Women committing online sexual abuse are always coerced by a male or are 'sick';
   d Online abuse by women has no serious impact on those affected; and
   e Boys enjoy online sex with women.

In the case of children and adolescents, specific messages can be part of existing programmes to promote safe and responsible Internet use. Given the significant extent of online grooming by females, and the likelihood that it gets concealed and overlooked,[87] special emphasis should be placed on raising awareness about females as perpetrators of sexual solicitation.[88]

2) Developing a series of measures and mechanisms to protect children from falling prey to both male and female sex offenders during their online interactions. This could include online safety tools on social networking sites such as chat moderation and report buttons, filtering software, guidelines and policies for companies providing APPs or online games to prevent their services from use in online sexual exploitation. Other possibilities are educational programmes and family guidelines promoting parental supervision, laws enhancing privacy protection, etc.

Secondary prevention strategies to reduce the risk of female-perpetrated online child sexual abuse and exploitation target the most vulnerable groups of victims and potential offenders. Measures in this area may include:

85 Doerner, Jill K. & Demuth, Stephen (2012), "Gender and sentencing in the Federal Courts: are women treated more leniently?", *Criminal Justice Policy Review* 20, n. 10 (2012): 1–28.

86 Riggio, Eliana and Hecht, Mark E. (2015), "Power, impunity and anonymity. Understanding the Forces Driving the Demand for Sexual Exploitation of Children", Bangkok: ECPAT International, accessed 12 December 2016, 74-76, http://www.ecpat.org/wp-content/uploads/2016/05/PowerImpunityandAnonymity.pdf.

87 Elliott, Ian A. and Ashfield, Sherry (2011), "The use of online technology", 10.

88 Schulz, Anja *et al.* (2016), "Online Sexual Solicitation of Minors", 181.

1) Educational programmes for high-risk children (e.g. those who may feel pressure to engage in sexting or are more vulnerable to online grooming such as girls that are exploring their sexual orientation, adolescents with low self-esteem or who are unhappy and in need, boys who may feel attractive by having the sexual attention of an older woman, etc.);

2) Implementing support schemes such as self-help programmes or counselling for women voluntarily identifying as at risk of offending;

3) Working with companies running dating websites to avoid their use as an entry point for online sexual abuse and exploitation by both male and female perpetrators; and

4) Making sure that both male and female teachers, nurses, volunteers, and others with access to children, are properly screened and children supervised in all at-risk professional settings.

Finally, tertiary prevention targets known female offenders to reduce recidivism and known victims to prevent re-victimisation. Actions under this axis of intervention may include:

1) Specialised helplines where victims can report incidents of female Internet sex offending and receive referral for further assistance;

2) Training for different target groups (law enforcers, teachers, parents, caregivers and other professionals) to improve capacities for identifying and supporting vulnerable children and child victims, and recognising possible signs of online abuse and exploitation.

   a. Capacity building for professionals should also aim at detecting and assisting females sexually offending through ICTs (this can be combined with awareness raising activities under primary prevention);

3) Ensuring treatment and monitoring of male known sex offenders, and where appropriate involving their partners, to prevent coercing women into online child sexual abuse and exploitation;

4) Anonymous counselling services (e.g. through helplines) where females concerned about their sexual interests in children can seek support (this may apply to both women at risk and those with prior offendes); and

5) Specialised treatment and management programmes for females engaging in online child sexual abuse and exploitation, including juvenile offenders.

With regard to points 3 and 4, there are already some successful initiatives targeting online sex offenders, including females, which could be replicated or adapted to other geographical/cultural contexts. One example is the Croga website (http://get-help.stopitnow.org.uk/), managed by the Lucy Faithfull Foundation in the UK, which provides free, anonymous self-help resources for people worried about downloading, viewing and using CSAMs. Another interesting initiative is the project "Inform", run by the same organisation which offers sound information, and emotional and practical support to wives, partners, adult family members and friends of people who have been arrested, cautioned or convicted in connection with accessing CSAMs on the Internet.[89]

Despite these positive examples, there still seems to be a lack of specialised programmes when it comes to the assessment and treatment of female Internet sex offenders. Generally speaking, research shows that what works for male offenders does not necessarily work for women and the diverse support needs of women require individual assessments which are gender responsive and must be informed by empirical research.[90]

In conclusion, these are only some interventions that can be designed and implemented to reduce and counteract female Internet sex offending. Recognising the harms posed by women committing child sex crimes in cyberspace is no longer avoidable. It is time to change societal structures that condone online sexual abuse and exploitation of children by this offender population and take action ensuring that child victims of this violation will not continue to remain unprotected and unheard.

89 The Lucy Faithfull Foundation, "Inform", accessed on 14 December 2016, http://ecsa.lucyfaithfull.org/sites/default/files/attachments/inform.pdf.

90 Cortoni, Franca and Gannon, Theresa A. (2013), "What works with female sexual offenders", in Craig, L., Dixon, L., & Gannon, T. A.

BIBLIOGRAPHY

Adams, Christine (1994), "Mothers Who Fail to Protect Their Children from Sexual Abuse: Addressing the Problem of Denial", Yale Law & Policy Review 12, n. 2 (1994): 519-539.

Alexy, Eileen M., Burgess, Anna W. & Baker, Thomas (2005), "Internet offenders: traders, travelers, and combination trader–travellers", *Journal of Interpersonal Violence* 20, n. 7 (2005): 804-12.

Babchishin, Kelly M., Hanson, R. Karl & Van Zuylen Heather (2015), "Online Child Pornography Offenders are Different: A Meta-analysis of the Characteristics of Online and Offline Sex Offenders Against Children", *Archives of Sexual Behavior* 44, n. 1 (2015): 45-66.

Babchishin, Kelly M., Hanson, Karl R., and Hermann, Chantal A. (2011), "The characteristics of online sex offenders: A meta-analysis", *Sexual Abuse: A Journal of Research and Treatment* 23, n.1 (2011): 92-123.

Beech, Anthony et al. (2009), "Assessing female sexual offenders' motivations and cognitions: an exploratory study", *Psychology, Crime & Law* 15, n. 2-3 (2009): 201-216.

Bexson, Laura (2011), "The ultimate betrayal – Female child sex offenders", *Internet journal of Criminology*, accessed on 15 November 2016, http://www.internetjournalofcriminology.com/Bexson_Female_Child_Sex_Offenders_IJC_July_2011.pdf.

Budd, Kristen M., Bierie, David M. & Williams, Katria (2015), "Deconstructing Incidents of Female Perpetrated Sex Crimes: Comparing Female Sexual Offender Groupings", *Sexual Abuse: A Journal of Research and Treatment*, published online before print July 10, 2015, DOI: 10.1177/1079063215594376.

Child Exploitation and Online Protection Center (2013), "Threat Assessment of Child Sexual Exploitation and Abuse 2013", London: CEOP, accessed 9 November 2016, https://ceop.police.uk/Documents/ceopdocs/CEOP_TACSEA2013_240613%20FINAL.pdf.

Child Exploitation and Online Protection Center (2012), "Threat Assessment of Child Sexual Exploitation and Abuse 2012", London: CEOP, accessed 9 November 2016, https://www.ceop.police.uk/Documents/ceopdocs/CEOPThreatA_2012_190612_web.pdf.

Cortoni, Franca, Babchishin, Kelly M.& Rat, Cleménce (2016), "The proportion of sexual offenders who are female is higher than thought. A meta-analysis", *Criminal Justice and Behavior.* Published online before print July 15, 2016, doi: 10.1177/0093854816658923. Abstract available at http://cjb.sagepub.com/content/early/2016/07/15/0093854816658923.abstract, accessed 9 November 2016.

Cortoni, Franca & Gannon, Theresa A. (2013), "What works with female sexual offenders", in Craig, L., Dixon, L., & Gannon, T. A. (Eds), *What works in offender rehabilitation: An evidence based approach to assessment and treatment* (pp. 271-284), Chichester, UK: Wiley-Blackwell.

Database of female sex offenders in UK and Ireland available at: https://theukdatabase.com/category/female-abuser/.

Database of Texas sex offenders available at http://www.texaspredators.com/SexOffendersByCrime.aspx.

Doerner, Jill K. & Demuth, Stephen (2012), "Gender and sentencing in the Federal Courts: are women treated more leniently?", *Criminal Justice Policy Review* 20, n. 10 (2012): 1–28.

Elliot, Ian A. & Beech, Anthony (2013), "The Psychological Profiles of Internet, Contact, and Mixed Internet/Contact Sex Offenders", *Sexual Abuse: A Journal of Research and Treatment Sex Abuse February* 25, n. 1 (2013): 3-20.

Elliott, Ian A., Ashfield, Sherry (2011), "The use of online technology in the modus operandi of female sex offenders", *Journal of Sexual Aggression* 17, n. 1 (2011): 1-13.

Elliot, Ian A. & Beech, Anthony (2009), "Psychological Profiles of Internet Sexual Offenders: Comparisons With Contact Sexual Offenders", *Sexual Abuse: A Journal of Research and Treatment* 21, n.1 (2009): 76-92.

EUROPOL- European Cybercrime Centre (EC3) (2013), "Commercial Sexual Exploitation of Children Online: A Strategic Assessment", 8, https://www.europol.europa.eu/publications-documents/commercial-sexual-exploitation-of-children-online.

Filetto, Giuseppe, “Baby squillo della Genova-Bene "Processate i clienti”, *La Repubblica,* 8 May 2016, accessed 5 December 2016, http://ricerca.repubblica.it/repubblica/archivio/repubblica/2016/05/08/baby-squillo-della-genova-bene-processate-i-clientiGenova07.html?ref=search.

Grayston, Alana D., & De Luca, Rayleen V. (1999), “Female perpetrators of child sexual abuse: A review of the clinical and empirical literature”, *Aggression and Violent Behavior* 4, n.1 (1999): 93–106.

Knox, P., “Revealed -The deep web: Where paedophiles like UK's worst Richard Huckle do as they please”, *Dailystar,* 6 June 2016, accessed 15 November 2016, http://www.dailystar.co.uk/news/latest-news/521079/dark-deep-web-tor-richard-huckle-hidden-paeophile-world.

Interagency Working Group on Sexual Exploitation of Children (2016), “Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse”, Bangkok: ECPAT International and ECPAT Luxembourg.

Lambert, Sharon & O’Halloran, Elaine (2008), “Deductive thematic analysis of a female paedophilia website”, *Psychiatry, Psychology and Law* 15, n. 2 (2008): 284–300.

Leukfeldta, Rutger E., Jansenb, Jurjen & Stol, Wouter P. (2014), “Child pornography, the Internet and juvenile suspects”, *Journal of Social Welfare and Family Law* 36, n. 1 (2014): 3-13.

López-Fonseca, Óscar, “Detenida por primera vez una mujer acusada de pedofilia”, *Publico*, 1 March 2011, accessed 15 November 2016, http://www.publico.es/espana/detenida-primera-vez-mujer-acusada.html.

Marcum, Catherine D., Higgins, George E. & Richard Tewksbury (2011), “Doing Time for Cyber crime: An Examination of the Correlates of Sentence Length in the United States”, *International Journal of Cyber Criminology* 5, n. 2 (2011): 824-835.

Martellozzo, Elena, Nehring, Daniel and Taylor, Helen (2010), “Online child sexual abuse by female offenders: An Exploratory study”, *International Journal of Cyber Criminology* 4, n. 1 & 2 (2010): 592–609.

Mathews, Frederick (1997), “The Invisible Boy: Revisioning the Victimization of Male Children and Teens”, Ottawa: National Clearinghouse on Family Violence.

McGuire, Mike & Dowling, Samantha (2013), “Cyber crime: A review of the evidence. Research Report 75. Chapter 3: Cyber-enabled crimes - sexual offending against children”, UK Home Office: London, accessed 10 November 2016, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246754/horr75-chap3.pdf.

Meter Onlus, “Meter Report 2014: bambini 0-3 anni sempre più coinvolti, un orrore senza fine crimini contro l’infanzia”, 5 March 2015, accessed 9 November 2016, http://www.associazionemeter.org/index.php/ct-menu-item-69/895-meter-report-2014-bambini-0-3-anni-sempre-piu-coinvolti-un-orrore-senza-fine-crimini-contro-l-infanzia.

Morris, Emma (2015), “#WePROTECT: Global Online Child Sexual Abuse Summit”, Policy Brief, accessed 9 November 2016, https://www.fosi.org/policy-research/weprotect-global-online-child-sexual-abuse-summit/.

Moya, Angel, “La pedófila que quería adoptar un niño”, *Telecinco,* 7 April 2011, accessed 15 November 2016, http://www.telecinco.es/informativos/sociedad/pedofila-queria-adoptar-nino_0_1200675158.html.

Nathan, Pamela & Ward, Tony (2002), “Female sex offenders: Clinical and demographic features”, *Journal of Sexual Aggression* 8, n. 1 (2002): 5–21.

New Zealand Department of Internal Affairs (2007), “Internet traders of child pornography: profiling research – update”, accessed 9 November 2016, https://www.dia.govt.nz/pubforms.nsf/URL/InternetTradersOfChildPornography-ProfilingResearchUpdate-February2007.pdf/$file/InternetTradersOfChildPornography.

NSPCC, “Unhealthy relationships highlighted in new Childline campaign”, 19 September 2016, accessed 12 December 2016, https://www.nspcc.org.uk/fighting-for-childhood/news-opinion/unhealthy-relationships-highlighted-new-childline-campaign/.

NSPCC, “Two sex offenders convicted a day for possession of child abuse images”, 22 July 2015, accessed 9 November 2016, https://www.nspcc.org.uk/fighting-for-childhood/news-opinion/huge-scale-of-online-child-abuse-images-revealed/.

Othmann, Hannah, "Police investigation launched after teenager is blackmailed by woman he met online", *Evening Standard,* 2 February 2016, accessed 15 November 2016, http://www.standard.co.uk/news/crime/police-investigation-launched-after-teenager-is-blackmailed-by-woman-he-met-online-a3171461.html.

Reconstruct, "What is known about female sex offenders and the impact on their victims?", accessed 16 November 2016, http://www.reconstruct.co.uk/public/docs/news/Female_sex_offenders.pdf.

Reijnen, Lotte, Bulten, Erik & Nijman, Henk (2009), "Demographic and Personality Characteristics of Internet Child Pornography Downloaders in Comparison to Other Offenders", *Journal of Child Sexual Abuse* 18 (2009): 611–622.

Riggio, Eliana & Hecht, Mark E. (2015), "Power, impunity and anonymity. Understanding the Forces Driving the Demand for Sexual Exploitation of Children", Bangkok: ECPAT International, accessed 12 December 2016, http://www.ecpat.org/wp-content/uploads/2016/05/PowerImpunityandAnonymity.pdf.

Robertson, Alexander, "Schoolgirl, 13, was abused by 137 paedophiles including a teacher after her profile was posted on a swingers website without her knowledge", *Daily Mail*, 12 August 2016, accessed 15 November 2016, http://www.dailymail.co.uk/news/article-3735760/Schoolgirl-13-abused-137-paedophiles-including-teacher-profile-posted-swingers-website-without-knowledge.html#ixzz4RIaKBvYy.

Rodríguez, Paco, "La Policía «caza» a la primera mujer pedófila española que actuaba en internet", *La Razon,* 4 March 2011, accessed 16 November 2016, http://www.larazon.es/historico/4569-una-quiosquera-y-un-inspector-de-hacienda-detenidos-por-pornografia-infantil-TLLA_RAZON_361522?sky=Sky-Noviembre-2016#Ttt10017ntRjL4s0.

Schulz, Anja et al. (2016) "Online Sexual Solicitation of Minors: How Often and between Whom Does It Occur?", *Journal of Research in Crime and Delinquency* 53, n.2 (2016): 165-188.

Seales, Rebecca, "Mother jailed after making 10-year-old daughter pose nude on Skype to enter fake $20,000 mom-child bikini shoot contest", *Daily Mail*, 1 March 2012, accessed 15 November 2016, http://www.dailymail.co.uk/news/article-2108565/Mother-jailed-making-10-year-old-daughter-pose-nude-Skype-enter-fake-20-000-mom-child-bikini-shoot-contest.html#ixzz4RIbyXQMA.

Seigfried-Spellar, Kathryn (2013), "Individual Differences of Internet Child Pornography Users: Peculiar Findings in a Community-Based Study", *International Journal of Cyber Criminology* 7, n. 2 (2013): 141-154.

Seigfried-Spellar Katherine C. and Rogers Marcus (2010), "Low neuroticism and high hedonistic traits for female internet child pornography consumers", *Cyberpsychology, Behavior and Social Networking* 13, n. 6 (2010): 629-35.

Seigfried, Kathryn C., Lovely, Richard W., & Rogers, Marcus K. (2008), "Self-reported online child pornography behaviour: A psychological analysis", *International Journal of Cyber Criminology* 2, n. 1 (2008): 286-297.

Simons, Dominique A. (2014), "Chapter 3: Sex Offender Typologies", in *Sex offender management, assessment and planning initiative,* eds. Holder, Eric H. Jr., Mason, Karol V. & de Baca, Luis C., Washington: U.S. Department of Justice - Office of Justice Programs.

Stathopoulos, Mary (2014), "Female sex offending and the gendered nature of sexual violence", Melbourne: Australian Institute of Family Studies, accessed 14 November 2016, https://aifs.gov.au/sites/default/files/publication-documents/ressum5.pdf.

The Lucy Faithfull Foundation, "Inform", accessed on 14 December 2016, http://ecsa.lucyfaithfull.org/sites/default/files/attachments/inform.pdf.

Wells, Melissa & Mitchell, Kimberly J. (2007), ''Youth Sexual Exploitation on the Internet: DSM-IV Diagnoses and Gender Differences in Co-occurring Mental Health Issues'', *Child and Adolescent Social Work Journal* 24 (2007): 235-60.

Williams, Katria S. & Bierie, David M. (2014), "An Incident-Based Comparison of Female and Male Sexual Offenders", *Sexual Abuse: A Journal of Research and Treatment,* published online on 30 July 2014, DOI: 10.1177/1079063214544333.

Wolak, Janis et al. (2014), "Trends in Unwanted Online Experiences and Sexting: Final Report. 2014", Durham, NH: Crimes against Children Research Center, accessed 9 November 2016, http://scholars.unh.edu/cgi/viewcontent.cgi?article=1048&context=ccrc.

Wolak, Janis, Mitchell, Kimberly and Finkelhor, David (2011), "Child Pornography Possessors: Trends in Offender and Case Characteristics", *Sexual Abuse: A Journal of Research and Treatment* 23, n. 1 (2011): 22-42.

Wolak, Janis, Mitchell, Kimberly & Finkelhor, David (2005), "Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study", National Center for Missing and Exploited Children: USA, accessed 9 November 2016, http://www.unh.edu/ccrc/pdf/jvq/CV81.pdf.

"23 women found guilty of child pornography", Radio Sweden, 18 October 2011, accessed 6 December 2016, http://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=4752927.

"Detienen mujer colombiana por grabar pornografia infantil con sus hijos", accessed 15 November 2016, http://www.ahoranoticias.cl/noticias/mundo/detienen-a-mujer-colombiana-por-grabar-pornografia-infantil-con-sus-hijos.html.

"L'Aquila: ricatto hard a minore, 200 Euro o metto foto in rete", 19 September 2016, accessed 15 November 2016, http://www.abruzzoweb.it/contenuti/l-aquila-ricatto-hard-a-minorenne-dammi-200-euro-o-metto-foto-in-rete-/610022-4/.

"MAKO/Files Online - Listing Australian Paedophiles/ Sex Offenders/ Child Killers", accessed 6 December 2016, http://www.mako.org.au/temp_female.html.

"Nursery sex abuse case: Profiles of Vanessa George, Colin Blanchard and Angela Allen", The Guardian, 1 October 2009, accessed 6 December 2016, https://www.theguardian.com/society/2009/oct/01/nursery-sex-case-abusers-profiles.

"Violenta una bambina scopre che è la figlia", *La Repubblica,* 18 November 2011, accessed 5 December 2016, http://ricerca.repubblica.it/repubblica/archivio/repubblica/2011/11/18/violenta-una-bambina-scopre-che-la-figlia.html?ref=search.

Live Streaming of Child Sexual Abuse: Background, Legislative Frameworks and the Experience of the Philippines

By: Andrea Varrella

INTRODUCTION

The use of information and communication technologies (ICTs) has grown dramatically in recent years with the widespread availability of Internet access on computers and mobile devices worldwide. While conducive to innovation, children's learning and development, the increased use of technology has downsides as well, including for the thousands of children exploited online every day.

Online predators now have a wide range of new and easier options for committing serious violations of the rights of the child. Hidden behind their computer screens and protected by the anonymity the technologies give them, offenders from all over the world can easily access children and sexually exploit them in ways no one would have ever imagined few years ago. Online sex offenders represent a particular category of sex offenders. Although they seemingly share common features with other sex offenders, those involved in online sexual crimes have been found to have higher professional and educational backgrounds, as well as a stronger history of social relationships; this could lead them to prefer non-contact because they may see them as less risky.[1]

This article focuses on the 'live streaming' of child sexual abuse, a form of child sexual exploitation (CSE) involving the participation of a child – by definition, under coercion - in sexual activities that are transmitted ('streamed') live on the Internet for potential viewing by hundreds, thousands or millions of people remotely.[2] While just one form of the wide range of video depictions of child sexual abuse (CSA) accessible online, live streaming is distinct as 'real-time' performance, with both attendant risks to victims and appeal to viewers as perpetrators.

This article explores and examines key aspects of this phenomenon – its definition, causes, consequences and the existing legislative international and national frameworks. Specific focus is given to the experience of the Philippines, from both a socio-cultural and a legislative point of view. Although the empirical evidence surrounding this issue is unreliable and still largely unknown, a recent proliferation of reported cases suggests that the Philippines is among the most significantly affected countries in the world.[3] This article asks the question: 'why?'; and offers recommendations for what is needed to better address this burgeoning scourge.

1 Chan, Eric J. MD, McNiel, Dale E. PhD, Binder, Renee L. MD (2016), "Sex offenders in the digital age", *The Journal of the American Academy of Psychiatry and the Law*, 44:368-375 citing Lee Austin F. *et al.* (2012), "Predictiing hands-on child sexual offenses among possessors of internet child pornography", *Psychology, Public Policy and Law*, 18:644-72, 16 April 2012.

2 ECPAT International (2015), "Factsheet on Live (streaming of) online child sexual abuse)", accessed 4 November 2016, http://www.ecpat.org/wp-content/uploads/2016/04/Live-abuse-via-webcam-Factsheet.pdf.

3 Brown, Andy (2016), "Safe from Harm: Tackling online child sexual abuse in the Philippines", UNICEF, accessed 11 November 2016, https://www.unicef.org/infobycountry/philippines_91214.html.

DEFINITION AND MAIN CHARACTERISTICS OF LIVE STREAMING OF CHILD SEXUAL ABUSE

The understanding and characterisation of live streaming of CSA continues to evolve, in the effort to keep pace with developments in technology, content and social and legal perspectives, albeit in a context of limited news articles, and reports and academic articles on this topic. Until recently, it was often referred to as 'webcam child sexual tourism'.[4] However, the recently adopted *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, reflecting the consultations of the Interagency Working Group on Sexual Exploitation of Children, point out that use of this term may lead to an inaccurate understanding and legislative loopholes.[5] The Guidelines recommend the terminology of 'live streaming of child sexual abuse', which can be used without stigmatising or otherwise harming the child.[6]

The live streaming of child sexual abuse combines two distinct manifestations of CSE in one crime: the production and transmission of child sexual abuse materials, and the exploitation of children in prostitution. Children are made to perform sexual acts alone or with other children or adults, which are captured and transmitted directly over the Internet. Perpetrators from anywhere with Internet connection can access the streamed video images.

Live streaming of child sexual abuse represents one type of the transmission and viewing of images of child sexual abuse using digital means, which also includes the much larger domain of recorded productions, as well as videogames, self-generated sexual content involving children and other forms. It must be emphasised at the outset that any and all child sexual abuse and exploitation is dangerous and completely unacceptable. However, live streaming is distinct in several respects making it particularly hazardous and offensive, as well as difficult to address.

First, the elements of risk and uncertainty attendant upon any live production may hold particular attraction for certain CSA perpetrators and thus, account for some part of the demand for this phenomenon. Second, the role of technology makes video increasingly easy to capture and transmit efficiently, and now accounts in its different forms for a massive share of all Internet traffic.

Live streaming does not require the actual downloading or storage of the abusive video footage or frames on a computer or personal electronic device. In principle, therefore, little or no trace of the crime remains, and offenders can more easily avoid detection by law enforcement officials. And unlike 'in-person' CSA in public settings such as bars or brothels, live streaming of CSA can be carried out in relative secrecy and the child victims can be moved from one hidden location to another so long as there is an Internet connection and a computer, smart phone or other broadcasting device.[7]

Often, overseas perpetrators can request certain sexual acts to take place in advance of the abuse, or while it is underway. The term 'child sexual abuse to order' has been used to highlight the active participation of viewers in deciding how the sexual act should be carried out.[8] However, even for those perpetrating and watching the crime without personally communicating or interfering, the lack of direct or active participation should not be considered

4 *See e.g.* Terre des Hommes (2013), "Webcam child sex tourism. Becoming Sweetie: A novel approach to stopping the global rise of Webcam Child Sex Tourism", 4 November 2011, accessed 2 November 2016, https://www.terredeshommes.nl/sites/tdh/files/uploads/research_report.pdf.

5 The emphasis on the relation between the perpetration of the crime and the tourist aspect could imply that the main available response lies within the tourism sector; and the inclusion of a specific technological device in the official nomenclature may result in a failure to recognise the crime when it is committed using other technologies. See: Interagency Working Group on Sexual Exploitation of Children (2016), "Terminology Guidelines for the protection of children from sexual exploitation and sexual abuse" (hereinafter Luxembourg Guidelines), adopted in Luxembourg on 28 January 2016, 48

6 Luxembourg Guidelines, 47.

7 International Justice Mission(2016), "IJM Casework Series – Cybersex Trafficking", accessed 3 November 2016, https://www.ijm.org/sites/default/files/IJM_2016_Casework_FactSheets_CybersexTrafficking.pdf.

8 Luxembourg Guidelines, 48.

a mitigating circumstance.

Similarly, the role of the perpetrator requesting and viewing the sex performance online should never be minimised. For example, the use of 'trendy' terminology such as 'virtual travelling sex offenders', may suggest that the offense is somehow less serious because of its 'non-contact' and transient nature.[9] By definition, child victims are abused by the facilitators ('offenders in loco') in order to satisfy the expected or communicated desires of the viewers. And in any case, 'viewing at a distance' is frequently not an isolated act: it has been found that there is a strong association between consumption of live-streamed child sexual abuse and subsequent travelling to sexually exploit the children in the country where they are located.[10]

Although live streaming is superficially a one-time, ephemeral transmission, the sexual activities streamed online may also be recorded, either by the perpetrator abroad or by the facilitator at the location of abuse. The videos can then be disseminated through darknets,[11] peer-to-peer networks[12] or other channels, substantially adding to the volume of child sexual abuse materials (CSAMs) available on the web as a whole.[13]

Usually, viewers of live streaming of CSA pay an amount of money to the facilitators or, more rarely, to the children themselves, through money transfer outlets, direct deposit to a bank account, or by using a virtual currency exchange.[14] Often, the flow of funds is the only evidentiary link between the perpetrator and the facilitator, although this can be further obscured through the use of encrypted money transfer systems. Other tracing mechanisms can be used, however, and evidence may also be provided by viewers' recordings of the performances. On the other side, the use of additional defensive methods, such as encryption, disposable email addresses, prepaid Internet access and disk-wiping technology, makes live streaming of child sexual abuse even harder to detect.[15]

The cost to produce and transmit live streaming of child sexual abuse is relatively low and thus, the prices charged to viewers are likely to be low, enabling perpetrators to access this kind of performance frequently.[16] Reportedly, the price for each single show varies depending on its length, the number and age of children, and the sexual acts that they perform. Usually the amount ranges between 500 and 2000 Philippine Pesos – PHP (currently equivalent to $10 – 40 USD[17]). When a facilitator is involved, child victims only receive a small amount, or nothing.[18]

9 European Financial Coalition against Commercial Sexual Exploitation of Children Online (2014), "Strategic assessment 2014", accessed 30 October 2016, https://www.europol.europa.eu/sites/default/files/publications/efc_strategic_assessment_2014.pdf.

10 EUROPOL (2016), "Internet Organised Crime Threat Assessment 2016 (IOCTA)", The Hague: European Police Office, 26, accessed 18 November 2016, https://static.rasset.ie/documents/news/europol-iocta-web-2016.pdf.

11 "Short for dark Internet, in file sharing terminology, a darknet is a Internet or private network, where information and content are *shared by darknet participants anonymously. Darknets are popular with users who share copy protected files as the service will let users send and receive files anonymously — that is, users cannot be traced, tracked or personally identified. Usually, darknets are not easily accessible via regular Web browsers.*" Beal, Vangie (n.d.), "Darknet", *Webopedia*, accessed 10 December 2016, http://www.webopedia.com/TERM/D/darknet.html.

12 "*Often referred to simply as peer-to-peer, or abbreviated P2P, peer-to-peer architecture is a type of network in which each workstation has equivalent capabilities and responsibilities. This differs from client/server architectures where some computers are dedicated to serving the others.*" Beal, Vangie (n.d.), "All about Peer-to- Peer (P2P) Networks, Webopedia, http://www.webopedia.com/DidYouKnow/Internet/peer_to_peer.asp.

13 EUROPOL (2016), IOCTA 2016, 26.

14 *For more information on this topic see*: Nouwen, Yvonne (2017), "Virtual currency uses for child sex offending online", ECPAT Journal issue 12.

15 The UK Database (n.d.), "Tech-savy paedophiles drive market for web-streamed child sex abuse", UK Database Online Sex Offenders Register, accessed 23 November 2016, https://theukdatabase.com/safety-tips-for-parents-children/tech-savvy-paedophiles-drive-market-for-web-streamed-child-sex-abuse/.

16 CEOP (2013), "Threat Assessment of Child Sexual Exploitation and Abuse", June 2013, accessed 10 November 2016, https://ceop.police.uk/Documents/ceopdocs/CEOP_TACSEA2013_240613%20FINAL.pdf.

17 Data retrieved from: XE Currency Converter, accessed 7 December 2016, http://www.xe.com/currencyconverter/convert/?Amount=1&From=PHP&To=USD.

18 European Financial Coalition against Commercial Sexual Exploitation of Children Online (2014), "Strategic assessment 2014".

Across all of its specific dimensions and features, it is certain that the live streaming of child sexual abuse represents a horrendous manifestation of online child sexual exploitation (OCSE); one that is apparently increasing in both scale and severity. For instance, in 2012, the Child Exploitation and Online Protection Centre (CEOP) of the UK's National Crime Agency (NCA) identified live streaming as an "*emerging* [emphasis added] method of indecent images of children's production and distribution".[19] Less than two years later, in 2014, the European Financial Coalition against Commercial Sexual Exploitation of Children Online defined the same phenomenon as an "*established* [emphasis added] trend".[20]

THE LEGAL FRAMEWORK AGAINST LIVE STREAMING OF CHILD SEXUAL ABUSE

International legal instruments

While the live streaming of child sexual abuse is not explicitly criminalised in any international convention or relevant legal standards, a number of these binding documents clearly recognise the formal illegality of the offending behaviours that are involved. As in many other areas, national policies, legislation and statutes would normally be developed based on the principles and/or the specific language of these international instruments.

First, Article 34 of the United Nations Convention on the Rights of the Child (CRC) requires States Parties to undertake all the appropriate measures to avoid "the exploitative use of children in prostitution, [...] other unlawful sexual practices, [and] in *pornographic performances* [emphasis added] and materials".[21] It should be clear that the 'shows' children are forced to perform in front of webcams are fully included in the "performances" cited in the Convention.

The Optional Protocol to the CRC on the sale of children, child prostitution and child pornography (OPSC), offers an even more specific protection for the victims of this distinct form of online child sexual abuse. The Protocol's Article 3(1.a.i) outlaws the "offering, delivering or accepting, by whatever means, [of] a child for the purpose of: (a) Sexual exploitation of the child",[22] and further forbids, *inter alia*, the act of producing, distributing, disseminating and selling of child pornography.[23] As stated in Article 2 of the OPSC, child pornography includes

> *"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".*[24]

Embracing a broader, and more protective interpretation of the provision, the sexual abuse perpetrated during the live streaming should be considered as a form of 'child pornography', even though the performance is not necessarily recorded and/or distributed, and is thus not necessarily aimed at disseminating new child sexual abuse materials online. However, as noted above, there is no reason that either the facilitator or the perpetrator cannot record and subsequently distribute the content that was live-streamed. In practical terms, it may not even

19 CEOP (2013), "Threat Assessment of Child Sexual Exploitation and Abuse", 8.

20 European Financial Coalition against Commercial Sexual Exploitation of Children Online (2014), "Strategic assessment 2014",22.

21 CRC, Article 34 (b and c).

22 UN General Assembly (2000), "Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography" (hereinafter OPSC), A/RES/54/263, 25 May 2000, entered into force on 18 January 2002, Article 3 (1.a.i).

23 OPSC, Article 3 (1.b).

24 OPSC, Article 2 (c).

be possible to ascertain that such steps have not been taken.

A similar legal disposition is contained in the International Labour Organisation (ILO) Convention No. 182 on the Worst Forms of Child Labour. This international instrument classifies the "use, procuring or offering of a child for prostitution, for the production of pornography or for pornographic performances" as among the worst forms of child labour, and urges State Parties to urgently take effective measures aimed at securing its prohibition and elimination.[25]

Analysing the wording of these three leading international legal instruments, it is apparent that the broader definitions conceived by the drafters, and approved by the respective State Parties, include the acts of both the perpetrators over the Internet and the facilitators *in loco* as existing within the scope of unacceptable behaviours. In turn, the referenced behaviours are interpreted and translated into national and transnational (e.g. EU) legislation.

One further convention is also highly relevant. As adopted by the Council of Europe (CoE), a regional intergovernmental organisation, the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (better known as Lanzarote Convention) opened for signatures in October 2007 and entered into force in July 2010.[26] In addition to its formal status for CoE member states, the Convention is open for signature by the non-member States which have participated in its elaboration, and by the European Union, and for accession by all the other non-member States.[27]

The Lanzarote Convention is the most advanced and complete legally binding standard at the international level in the field of sexual exploitation and sexual abuse of children. It focuses on substantive and procedural criminal legal measures in order to define and criminalise SEC-related crimes, prosecute perpetrators, promote appropriate national policies, as well as provide specific measures for the protection of child victims. The Lanzarote Convention complements the other relevant international instruments – the CRC, the OPSC and Convention No. 182 – by, among other things, providing a legal framework which identifies some manifestations of CSEC that are not included in the UN instruments, such as the solicitation of children for sexual purposes through information and communication technologies (online grooming).

Also of relevance for present purposes, the Lanzarote Convention contains a specific article criminalising all actions concerning the participation of a child in pornographic performances.[28] As stated in Article 21(1), State Parties should:

> *"Ensure that the following intentional conduct is criminalised: a. recruiting a child into participating in pornographic performances or causing a child to participate in such performances; b. coercing a child into participating in pornographic performances or profiting from or otherwise exploiting a child for such purposes; c. knowingly attending pornographic performances involving the participation of children."*

25 International Labour Organisation (1999), "Worst Forms of Child Labour Convention (No. 182)" (hereinafter Convention No. 182), entered into force on 19 November 2000, Article 3(b).

26 The Convention has been signed by all 47 of the CoE's member states and ratified by 42 of the states. https://www.coe.int/en/web/children/lanzarote-convention

27 "'Accession' is the act whereby a state accepts the offer or the opportunity to become a party to a treaty already negotiated and signed by other states. It has the same legal effect as ratification." United Nations Treaty Collection, "Glossary of terms relating to treaty actions", accessed 25 November 2016, https://treaties.un.org/pages/Overview. aspx?path=overview/glossary/page1_en.xml#accession.

28 Council of Europe (2007), "Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse" (hereinafter Lanzarote Convention), signed on 25th October 2007, entered into force on 1st July 2010, Article 21.

This international convention thus explicitly recognises the unlawfulness of a range of conducts concerning live streaming of CSA for both the perpetrator (viewer) and the facilitators.

In summary, although there is a lack of explicit criminalisation of live streaming of child sexual abuse in the relevant international instruments, a number of provisions in these instruments can be applied to capture the severe level of criminality and illegality of this recent and alarming OCSE-related offense, and guide appropriate national-level action.

National legislation in the Philippines

The Philippines represent an important case study for the application of the above international instruments in national laws and policies. As the Philippines ratified the CRC in 1990,[29] the OPSC in 2002[30] and the ILO Convention No. 182 in 2000,[31] its national legislation is required to comply with their provisions. The Philippines is currently the only country in South East Asia considering accession to the Lanzarote Convention.[32] Comparing the national legislation on OCSE of all the countries in the region, the Philippines' legal framework has been found to be the most comprehensive and in compliance with the international standards.

This process began in 1992, when the Congress of the Philippines passed its first act specifically aimed at preventing child abuse, exploitation and discrimination and protecting child victims; commonly known as Special Protection of Children against Abuse, Exploitation and Discrimination Act.[33] Article V of this act imposes imprisonment for hiring, employing, using, persuading, inducing and coercing children to take part in "obscene exhibitions and indecent shows".[34] The proscription is very comprehensive, insofar as it includes exhibitions and shows performed live or on video. As the first webcams only entered the market place after the adoption of the act, the lack of mention of the possibility for a show to be performed 'live' and 'on video' should not be considered as a gap, but instead a sign of the urgent need, worldwide, to devise domestic legislation effectively meeting the evolving challenges faced by governments in the digital era.

The Anti-Child Pornography Act, adopted in 2009, finally made illegal child sexual abuse materials in the Philippines, and enumerated a number of related crimes. Section 4 of the Act appears to be applicable to the live streaming of child sexual abuse, including one part which declares the unlawfulness of using, persuading, inducing and coercing "a child to perform in the creation or production or any form of child pornography"[35] and, specifically, broadcasting it.[36] A few lines below, the article prohibits the willful access to any form of 'child pornography'.[37] As per the Act's definition,

29 United Nations Treaty Collection (n.d.), "Status of treaties: Convention on the Rights of the Child", accessed 3 December 2016, https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-11&chapter=4&clang=_en.

30 United Nations Treaty Collection (n.d.), "Status of treaties: OPSC", accessed 3 December 2016, https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-11&chapter=4&clang=_en.

31 ILO (n.d.), "Ratifications of C182- Worst Forms of Child Labour Convention, 1999 (No. 182)", accessed 3 December 2016, http://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:11300:0::NO::P11300_INSTRUMENT_ID:312327.

32 UNICEF (2016), "Child Protection in the Digital Era. National responses to online child sexual abuse and abuse in ASEAN Member States", Bangkok: UNICEF EAPRO, 15, accessed 30 November 2016, https://www.unicef.org/eapro/Child_Protection_in_the_Digital_Age.pdf.

33 Republic of the Philippines (1992), "An act providing for stronger deterrence and special protection against child abuse, exploitation and discrimination, and for other purposes", Republic Act No. 7610, 17 June 1992.

34 *Ibid*., Article V.

35 Republic of the Philippines (2009), "An act defining the crime of child pornography, prescribing penalties therefor and for other purposes (Anti- Child Pornography Act of 2009)", Republic Act No. 9775, §4 (a).

36 *Ibid*., §4 (c).

37 *Ibid*., §4 (j).

> *" 'child pornography' refers to any representation, whether visual, audio, or written combination thereof, by electronic, digital optical, magnetic or any other means, of child engaged or involved in real or simulated explicit sexual activities".*[38]

This law could be used to prosecute both the facilitators broadcasting the sexual abuse and the viewers, in country or abroad, accessing the video material.

A further step forward in the protection of children against sexual exploitation online was made in 2012 when the Cybercrime Prevention Act entered into force. According to section 4 (c), legislating content-related cybercrimes, the punishment applicable to the acts prohibited by the Anti-Child Pornography Act must be increased by one degree, in accordance with the penalties duration's scale provided by Chapter III of the Revised Penal Code,[39] if committed using a computer system.[40]

Both the Special Protection of Children against Abuse, Exploitation and Discrimination Act and the Anti-Child Pornography Act provide a definition of the child, referring to any person below 18 years of age or over 18 years of age but unable to take care of and protect himself/herself.[41] Hence, these two pieces of legislation appear adequate and in compliance with Article 1 of the CRC.[42]

Unfortunately, however, this is not the case for the more general provision stating the age of consent for girls. According to Article 335 of the Revised Penal Code, the age of consent for girls is 12 years of age. Specifically, the mentioned article outlaws rape under three different circumstances: "1. By using force or intimidation; 2. When the woman is deprived of reason or otherwise unconscious; and 3. When the *woman* is under twelve years of age [emphasis added], even though neither of the circumstances mentioned in the two next preceding paragraphs shall be present".[43]

While international legal instruments do not recommend an explicit age of consent, the Committee on the Rights of the Child stated in its General Comment No. 4 on adolescent, health and development, that States need to set a minimum age for sexual consent without any gender differences and that takes into account "the recognition of the status of human beings under 18 years of age as rights holders, in accordance with their evolving capacity, age and maturity (arts. 5 and 12 to 17 of the CRC)."[44]

Compared with similar provisions in the legislation of other countries, the Philippines has the lowest age of consent in the region.[45] This provision weakens the protection of child victims of CSEC-related crimes and the prosecution of their abusers; specifically, in the case of lack of application of the Anti-Child Pornography Act and Cyber Crime Act, girls above 12 years of age who are abused cannot be considered as victims of statutory rape.

---

38 *Ibid*., §3 (b).

39 Republic of the Philippines (1930), "An act revising the penal code and other penal laws (The Revised Penal Code)", Act No. 3815, 8 December 1930, Chapter III, Section I "Duration of Penalties".

40 Republic of the Philippines (2012), "An act defining cybercrime, providing for the prevention, investigation, suppression and the imposition of penalties therefor and for other purposes (Cybercrime Prevention Act of 2012)", Republic Act No. 10175, §4 (c)(2).

41 Special Protection of Children against Abuse, Exploitation and Discrimination Act, §3(a); Anti-Child Pornography Act, §3(a).

42 CRC, Article 1.

43 Republic of the Philippines (1930), The Revised Penal Code, Article 335 "Rape and Acts of Lasciviousness".

44 Committee on the Rights of the Child (2003), "Adolescent Health and Development in the Context of the Convention on the Rights of the Child" General Comment No.4, UN Doc. CRC/GC/2003/4,

45 UNICEF (2015), "Legal Protection from Violence Analysis of Domestic Laws Related to Violence against Children in ASEAN Member States", Bangkok: UNICEF EAPRO, accessed 17 January 2017, https://www.unicef.org/eapro/ASEAN_VAC(1).pdf. 1 July 2013, accessed 17 January 2017, http://www.refworld.org/docid/4538834f0.html.

In summary, the Philippines adopted generally comprehensive and high-quality legislation addressing child sexual exploitation in line with the relevant international legal instruments, which is seen to be applicable to the live streaming of CSA. A major exception arises, however, in regard to the weak definition of the age of consent.

WHY THE PHILIPPINES? SOCIO-CULTURAL AND ECONOMIC FACTORS

In the context of this strong and applicable national legislation, it may seem paradoxical that the Philippines has recently been described as "the global epicentre of the live-stream sexual abuse trade".[46] According to a journalistic investigation carried out in 2015, there were 167 ongoing, live-streaming criminal cases in the Philippines (57 raised in 2013 and 80 in 2014).[47] However, as discussed above, the live streaming of CSA leaves almost no trace and the number of criminal cases undoubtedly understates the reality. At the same time, there remains a lack of reliable data on the scale of the phenomenon in every country. But according to the latest estimates, tens of thousands of children are victimised by this form of exploitation in the Philippines.[48]

Several interrelated facilitating factors may be seen to explain the apparent high concentration of live streaming of CSA in this country of some 103 million population. Against the overall strong record of economic development in the Philippines, relatively high levels of poverty provide a socioeconomic context for the proliferation of child sexual exploitation and abuse within parts of the population. The incidence of economic poverty among Filipinos was officially reported as 26.3% in the first six months of 2015,[49] meaning that about one-quarter of the families in the Philippines live under the poverty line.[50]

Poverty in the Philippines, as in many other countries, is not only economic. The value for the Philippines on the UNDP's Multidimensional Poverty Index for 2015 was 0.033,[51] signalling the simultaneous presence of multiple significant deprivations in addition to financial hardship.[52] Many people living in the slums of the biggest cities in the Philippines are unemployed or have unstable jobs. Evidence from different sources points to the reality that children and adults sexually exploited and abused on a transactional basis are members

46 Brown, Andy (2016), "Safe from Harm: Tackling online child sexual abuse in the Philippines".

47 Holmes, Oliver (2016), "How child sexual abuse became a family business in the Philippines", *The Guardian*, 31 May 2016, accessed 8 November 2016, https://www.theguardian.com/world/2016/may/31/live-streaming-child-sex-abuse-family-business-philippines.

48 Terre des Hommes (n.d.), " WCST FAQ – WCST as a phenomenon", accessed 17 November 2016, http://www.terredeshommes.org/wp-content/uploads/2013/11/FAQ-English.pdf.

49 Philippine Statistics Authority (2016), "Poverty incidence among Filipinos registered at 26.3 %, as of first semester of 2015 – PSA", 18 March 2016, accessed 2 November 2016, https://psa.gov.ph/content/poverty-incidence-among-filipinos-registered-263-first-semester-2015-psa.

50 Mendoza, Ronal U., Olfindo, Rosechin, Maala, Camila Regina (2016), "Spatial disparities and poverty: The Case of three Provinces in the Philippines", *Ateneo School of Government Working Paper Series*, September 2016, accessed 3 December 2016, https://poseidon01.ssrn.com/delivery.php? https://poseidon01.ssrn.com/delivery.php? D=882123066117005090064028006017012104017037064079033004076088091068091113087007124000036041017035040124044000112070007070003072038045044040053067030005096116125102056022083115124067121028117097085093004102118003 09.

51 UNDP (2015), "Human Development Report 2015 – Work for Human Development", New York: UNDP, 229, accessed 7 December 2016, http://hdr.undp.org/sites/default/files/2015_human_development_report_1.pdf. "The Multidimensional Poverty Index (MPI) complements monetary measures of poverty by considering overlapping deprivations suffered at the same time. The index identifies deprivations across the same three dimensions as the HDI and shows the number of people who are multi-dimensionally poor (suffering deprivations in 33% or more of weighted indicators) and the number of deprivations with which poor households typically contend with." UNDP (n.d.), "Multidimensional Poverty Index (MPI)", UNDP's website, accessed 7 December 2016, http://hdr.undp.org/en/content/multidimensional-poverty-index-mpi.

52 "The Multidimensional Poverty Index (MPI) identifies multiple deprivations at the household and individual level in health, education and standard of living. It uses micro data from household surveys, and—unlike the Inequality-adjusted Human Development Index—all the indicators needed to construct the measure must come from the same survey. Each person in a given household is classified as poor or non-poor depending on the number of deprivations his or her household experiences. These data are then aggregated into the national measure of poverty." UNDP, "Frequently Asked Questions: Multidimensional Poverty Index (MPI)", accessed 7 December 2016, http://hdr.undp.org/en/faq-page/multidimensional-poverty-index-mpi#t295n2429.

of the poorer segments of society, with limited income earning options. Within this group, some adults and children are likely to be attracted by the possibility to earn a little money by streaming online sexual performances to be viewed by wealthy westerners, regardless of the possible consequences. Poverty of course, affects many countries, and the Philippines is by far not among the poorest countries in the world.

But a second important feature of the Philippines facilitating its prominence in the live streaming of CSA, is the widespread use of English language among its citizens. As one of the two official languages (along with Filipino), English is spoken by more than 14 million citizens.[53] According to the Education First English Proficiency Index (EPI), ranking world's countries by English language skills, the Philippines ranks 13th and it is included among the countries with a very high English proficiency.[54]

As English has come to serve as a global lingua franca, particularly in wealthier parts of the world where many perpetrators of child sexual abuse can afford to pay for live streaming and other digital services. Child victims, facilitators and viewers are therefore able to communicate via email, videoconferencing and instant messages before, during and after the perpetration of the crime. Offenders can remotely dictate and control the actions of the children and abusers with few language barriers.

Third, availability of technology and easy access to the Internet further contribute to the live streaming of child sexual abuse in the Philippines. According to the ICT Development Index 2016 of the International Telecommunication Union, 27 percent of households in the Philippines have a computer.[55] Internet usage is extremely high, placing the Philippines among the top 20 countries in the world in terms of the number of Internet users.[56] Fifty four million Filipinos (some 53 % of the population) have access to the web through different channels,[57] and use of the Internet is growing rapidly.[58]

A noteworthy aspect of computer and Internet availability in the Philippines is their use by children. According to a recent survey conducted by the London School of Political Science (LSE) and UNICEF, "in the Philippines, over three-quarters of surveyed children (76 per cent) use free Internet when they can and 41 per cent of children use pay as you go Internet [...]. About one-third of children (29 percent) use prepaid Internet to connect."[59] The most common devices used by Filipino children to go online are smart phones, followed by tablets, games consoles and finally, desktop or laptop computers.[60]

Devices are generally relatively affordable, and are sought after by children in all income groups. Even when devices are not available at home or school, the Internet can be affordably accessed through a new business model gaining ground in the last few years: Piso Net, a chain of Internet cafes charging per minute rather than hourly.

---

53 Cabigon, Mike (n.d.), "State of English in the Philippines: Should we be concerned?", accessed 3 November 2016, https://www.britishcouncil.ph/teach/state-english-philippines-should-we-be-concerned-2.

54 EF (2016), "The world's largest ranking by English skills – sixth edition", EF's website, accessed 3 December 2016, http://www.ef.co.th/epi/.

55 ITU (2016), "ICT Development Index 2016", *ITU's website*, accessed 1 December 2016, http://www.itu.int/net4/ITU-D/idi/2016/#idi2016countrycard-tab&PHL.

56 Internet World Stats (2016), "Top 20 countries with the highest number of Internet users", *Internet World Stats – Usage and Population Statistics*, accessed 8 December 2016, http://www.internetworldstats.com/top20.htm.

57 Ibid.

58 Internet World Stats (2016), "Philippines, Internet usage stats and marketing report", *Internet World Stats – Usage and Population Statistics*, accessed 8 December 2016, http://www.internetworldstats.com/asia/ph.htm.

59 Byrne, Jasmina et al. (2016), "Global Kids Online – Research Synthesis 2015-2016", November 2016, UNICEF Office of Research – Innocenti and London Schools of Economics and Political Science, 28, accessed 29 November 2016, http://blogs.lse.ac.uk/gko/wp-content/uploads/2016/11/Synthesis-report_07-Nov-2016.pdf.

60 *Ibid*., 31.

One Philippine Peso (two U.S. cents) provides four minutes online.[61] Children in the Philippines are thus likely to be familiar with the devices and processes for live streaming of abuse, which may weaken potential barriers to the practice.

A fourth distinctive feature of the Philippines facilitating financial transactions around live streaming of CSA is the well-established, money transfer system which has been developed in large part to support remittances by emigrant Filipino workers. Many Filipinos work for several months or even all year long in other countries in the region, as well as in Europe and the US. In 2013, the Commission on Filipinos Overseas estimated that approximately 10 million Filipinos were working abroad on either a permanent, temporary or an irregular basis.[62] The need to send money that was earned back to their families at home has led to the development of a dense network of money transfer outlets across the country, including more than 600 Western Union agents in Manila alone.[63] These same services simplify payments by viewers of the live streaming of child sexual abuse.

A final, crucial feature in the Philippines situation which may be inferred from available evidence is, in many cases, an apparent absence of perceived conflict between the live streaming of CSA and relevant social norms. The persons facilitating the practice are often found to be members of the community, parents and relatives of the child victims – the primary duty-bearers responsible for promoting the best interest of the child.[64]

According to the International Justice Mission, in more than half of its cases related to the live streaming of CSA, "the criminal profiting from the abuse is a parent, relative or close family friend".[65] During a 2014 police raid in Manila, authorities found a group of children aged between 7 and 10 preparing for a sexual performance under the supervision of the mother of one of the children. The other three children were also living with the woman while their mother worked outside the city.[66]

Complete data is not available for either the relationships between the facilitators of live streaming of child sexual abuse and the child victims, or their understanding of relevant norms and standards in the Philippines and other countries. However, if the above findings are even partially accurate, they carry several significant implications. The acceptance and facilitation of live streaming of child sexual abuse by community and family members may be due to – but is not justified by – a lack of awareness and knowledge about the harm that the acts cause to children, and about the unlawfulness of the practice. Reportedly, some parents in the Philippines do not consider what they are doing to their children abusive because the offender, being far away, does not actually touch them.[67] It is thus possible that such behaviours are seen by some as acceptable, and that sexual exploitation of children online is justified and may even be fostered within the family and the community of belonging and identity. The involvement of parents and relatives in the perpetration of the crime and the likely existence of social norms justifying has a further consequence, namely that children may feel guilty for accusing or testifying against them. To protect their parents,

61 ABS-CBN News (2013), "P1 Internet service is a hot new business in PH", *ABS-CBN News*, 15 February 2013, accessed 20 November 2016, http://news.abs-cbn.com/business/02/15/13/p1-internet-service-hot-new-business-ph.

62 Office of the President of the Philippines – Commission on Filipinos Abroad (n.d.), "Yearly Stock Estimation of Overseas Filipinos", accessed 1 December 2016, http://www.cfo.gov.ph/program-and-services/yearly-stock-estimation-of-overseas-filipinos.html.

63 Western Union (n.d.), "Find Locations", *Western Union's website*, accessed 8 December 2016, https://locations.westernunion.com/search/philippines/ncr/manila?page=81&q=country%3APH%3Bcity%3AManila.

64 UN General Assembly (1989), "Convention on the Rights of the Child" (hereinafter CRC), Res. 44/25 of 20 November 1989, entered into force on 2nd September 1990, article 3 (2).

65 IJM (2016), "IJM's first conviction in a live-streaming cybersex trafficking case", *Newsroom*, 10 August 2016, accessed 3 November 2016, http://news.ijm.org/ijms-first-conviction-in-a-live-streaming-cybersex-trafficking-case/?_ga=1.57678313.297016410.1481190992.

66 Brown, Andy (2016), "Safe from Harm: Tackling online child sexual abuse in the Philippines".

67 TheUKdatabase (n.d.), "Tech-savy paedophiles drive market for web-streamed child sex abuse".

children may lie, refuse to speak, or deny anything happened to them,[68] thus magnifying the psychological costs and perpetuating the practice.

Taken together, a context of poverty affecting a large part of the national population; common use of the English language; widespread access to and use of computers and the Internet; a well-functioning money transfer system; and potential perception of a lack of conflict with relevant norms and laws offer valid explanations for the reported prevalence of live streaming of child sexual abuse in the Philippines. The evidence in each of these areas is limited however, and in the absence of complete data, this discussion should be seen as only opening a reflection on the complexity of this practice and its embeddedness in society – despite the presence of a generally highly satisfactory legal framework. In addition, it suggests directions for further investigation of this problem in the Philippines, and the steps that may be taken to address it.

CONCLUSIONS AND RECOMMENDATIONS

The live streaming of child sexual abuse is a trend likely to accelerate in many parts of the world because of its essential characteristics on the side of both supply and demand: ease of access; availability of the devices needed to perpetrate the crime; easily generated income for facilitators and children; low risk levels for being caught by law enforcement; low costs of production; and low costs to view the performances.

The overview of the main international legal instruments relevant to the sexual exploitation of children provides an up-to-date picture of international law applicable to this OCSE crime. The ensuing obligations of States are identifiable, as well as the need for specific national legislation against online child sexual exploitation. International and national standards require several adjustments and refinements in order to better align with the current context of the online child sexual exploitation, which has been overwhelmed by the availability and affordability of new technologies.

The case of the Philippines is highly pertinent. The country took strong and exemplary measures against the live streaming of child sexual abuse with the adoption of the Anti-Child Pornography Act and the Cybercrime Prevention Act, the creation of a specialised Office of Cybercrime and constructive cooperation with Interpol and other international organisations.[69]

Unfortunately, the concentration of live streaming of child sexual abuse related cases in the Philippines casts a shadow over the positive developments of a robust legal framework, policies and interventions. The available evidence suggests that domestic legal protection and a regulatory framework alone are not sufficient to address this multi-faced phenomenon, particularly in light of its intrinsic nature, its newness and some of its key features making it both easy to spread, and problematic to document.

As described, these include a context of poverty affecting much of the population, use of English, availability of technology and facilitating systems, and potential misperceptions concerning harm to the minds of children, parents and local communities. These interacting factors are distinctively relevant to the Philippines, but they are present in varying degrees in many other countries around the world, indicating that this practice is not unique to one country.

The live streaming of child sexual abuse represents a distinctive and disturbing manifestation of the wider prevalence of child sexual abuse and exploitation, including its online forms. Accordingly, the steps required to address it include a combination of continuing general efforts against CSA, along with tailored actions addressing the specific features of live streaming of child sexual abuse. To the extent that an adequate legal framework is not yet in place, priority must be placed on its development.

68 *Ibid*.

69 Brown, Andy (2016), "Safe from Harm: Tackling online child sexual abuse in the Philippines".

In the Philippines and many other countries such a framework is established, and the challenge is to bridge the gap between legal provisions and their effective enforcement. The phenomenon of live streaming of child sexual abuse must be tackled on many different fronts and with the involvement of many diverse actors. Awareness-raising activities in schools and communities for both children and parents are needed to reinforce social norms that are in line with the rights of the child and to correct distorted perceptions concerning the illegality and manifold harms of sexual activities that do not involve contact by the ultimate perpetrator, the viewer. Concerted and coordinated activities as well as investigative efforts of national law enforcement units and relevant private actors are also likely to lead to more positive results. For instance, close collaboration with financial institutions and financial services companies may help law enforcement to identify perpetrators and children at risk by tracking suspicious transactions and money deposits.

The involvement and commitment of Internet Service Providers (ISPs), especially those offering web-hosting services, may offer the possibility to monitor chatrooms and other online platforms reportedly used by perpetrators to make the first contact with potential victims and facilitators. In these cases, the local police would be able to collect the evidence needed to begin investigative operations or build cases against perpetrators.

For instance, numerous reports have been submitted to the Philippines Office for Cybercrime by US Electronic Service Providers (ESPs) and ISPs, highlighting the potential to track offences. Also in the Philippines, national mechanisms for reporting child sexual abuse materials (such as through phone calls, emails and SMS) have been implemented by several governmental offices and divisions.[70] Because live streaming of child sexual abuse is predominantly viewed across national borders, productive collaboration at many different levels between national authorities of different countries, and with relevant international organisations, is a paramount requirement for effective response.

This article aimed to provide a rounded picture of why the Philippines is fertile ground for the live streaming of child sexual abuse. It also illustrates what child protection specialists have always argued, namely: that robust legal frameworks, while absolutely important, are not sufficient in themselves to address and prevent the different manifestations of sexual abuse of children.

Further research and documentation, as well as cooperation and information-exchange between the various actors in the field, is needed to inform future strategies against live sexual abuse of children and to enhance our understanding of why it persists despite many positive developments and strong efforts against it at the national level. The strategy of the Philippines against live streaming of child sexual abuse is a proactive example that will undoubtedly produce better positive results in the near future, and that should guide the development of effective and comprehensive legislation and policies worldwide.

70 Republic of the Philippines – Department of Justice (2015), "Advisory in online Child Abuse", 28 August 2015, accessed 25 January 2017, https://www.doj.gov.ph/files/cybercrime_office/Advisory%20on%20Online%20Child%20Abuse.pdf.

BIBLIOGRAPHY

ABS-CBN News (2013), "P1 Internet service is a hot new business in PH", ABS-CBN News, 15 February 2013, accessed 20 November 2016, http://news.abs-cbn.com/business/02/15/13/p1-internet-service-hot-new-business-ph.

Beal, Vangie (n.d.), "All about Peer-to- Peer (P2P) Networks, Webopedia, http://www.webopedia.com/DidYouKnow/Internet/peer_to_peer.asp.

Beal, Vangie (n.d.), "Darknet", Webopedia, accessed 10 December 2016, http://www.webopedia.com/TERM/D/darknet.html.

Beal, Vangie (n.d.), "Streaming", Webopedia, accessed 10 November 2016, http://www.webopedia.com/TERM/S/streaming.html.

Brown, Andy (2016), " Safe from Harm: Tackling online child sexual abuse in the Philippines", UNICEF, accessed 11 November 2016, https://www.unicef.org/infobycountry/philippines_91214.html.

Byrne, Jasmina et al. (2016), "Global Kids Online – Research Synthesis 2015-2016", November 2016, UNICEF Office of Research – Innocenti and London Schools of Economics and Political Science, 28, accessed 29 November 2016, http://blogs.lse.ac.uk/gko/wp-content/uploads/2016/11/Synthesis-report_07-Nov-2016.pdf.

Cabigon, Mike (n.d.), "State of English in the Philippines: Should we be concerned?", accessed 3 November 2016, https://www.britishcouncil.ph/teach/state-english-philippines-should-we-be-concerned-2.

CEOP (2013), "Threat Assessment of Child Sexual Exploitation and Abuse", June 2013, accessed 10 November 2016, https://ceop.police.uk/Documents/ceopdocs/CEOP_TACSEA2013_240613%20FINAL.pdf.

Chan, Eric J. MD, Mc Niel, Dale E. PhD, Binder, Renee L. MD (2016), "Sex offenders in the digital age", The Journal of the American Academy of Psychiatry and the Law, 44:368-375.

Committee on the Rights of the Child (2003), "Adolescent Health and Development in the Context of the Convention on the Rights of the Child" General Comment No.4, UN Doc. CRC/GC/2003/4, 1 July 2013, accessed 17 January 2017, http://www.refworld.org/docid/4538834f0.html.

Council of Europe (2007), "Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse" (hereinafter Lanzarote Convention), signed on 25th October 2007, entered into force on 1st July 2010, Article 21.

ECPAT International (2015), "Factsheet on Live (streaming of) online child sexual abuse)", accessed 4 November 2016, http://www.ecpat.org/wp-content/uploads/2016/04/Live-abuse-via-webcam-Factsheet.pdf.

EF (2016), "The world's largest ranking by English skills – sixth edition", EF's website, accessed 3 December 2016, http://www.ef.co.th/epi/.

European Financial Coalition against Commercial Sexual Exploitation of Children Online (2014), "Strategic assessment 2014", accessed 30 October 2016, https://www.europol.europa.eu/sites/default/files/publications/efc_strategic_assessment_2014.pdf

EUROPOL (2016), "Internet Organised Crime Threat Assessment 2016 (IOCTA)", The Hague: European Police Office, 26, accessed 18 November 2016, https://static.rasset.ie/documents/news/europol-iocta-web-2016.pdf.

Global Kids Online (2016), " Global Kids Online, the Philippines, Executive Summary", November 2016, 4, accessed 29 November 2016, http://blogs.lse.ac.uk/gko/wp-content/uploads/2016/02/Executive-summary_28-Oct-2016.pdf.

Holmes, Oliver (2016), "How child sexual abuse became a family business in the Philippines", The Guardian, 31 May 2016, accessed 8 November 2016, https://www.theguardian.com/world/2016/may/31/live-streaming-child-sex-abuse-family-business-philippines?platform=hootsuite.

IJM (2016), "IJM's first conviction in a live-streaming cybersex trafficking case", Newsroom, 10 August 2016, accessed 3 November 2016, http://news.ijm.org/ijms-first-conviction-in-a-live-streaming-cybersex-trafficking-case/?_ga=1.57678313.297016410.1481190992.

ILO (n.d.), "Ratifications of C182- Worst Forms of Child Labour Convention, 1999 (No. 182)", accessed 3 December 2016, http://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:11300:0::NO::P11300_INSTRUMENT_ID:312327.

Interagency Working Group on Sexual Exploitation of Children (2016), "Terminology Guidelines for the protection of children from sexual exploitation and sexual abuse" (hereinafter Luxembourg Guidelines), adopted in Luxembourg on 28 January 2016, 48.

International Justice Mission (2016), "IJM Casework Series – Cybersex Trafficking", accessed 3 November 2016, https://www.ijm.org/sites/default/files/IJM_2016_Casework_FactSheets_CybersexTrafficking.pdf.

International Labour Organisation (1999), "Worst Forms of Child Labour Convention (No. 182)" (hereinafter Convention No. 182), entered into force on 19 November 2000, Article 3(b).

Internet World Stats (2016), "Myanmar, Internet usage, broadband and telecommunications reports", Internet World Stats – Usage and Population Statistics, accessed 8 December 2016, http://www.internetworldstats.com/asia/mm.htm.

Internet World Stats (2016), "Philippines, Internet usage stats and marketing report", Internet World Stats – Usage and Population Statistics, accessed 8 December 2016, http://www.internetworldstats.com/asia/ph.htm.

Internet World Stats (2016), "Top 20 countries with the highest number of Internet users", Internet World Stats – Usage and Population Statistics, accessed 8 December 2016, http://www.internetworldstats.com/top20.htm.

ITU (2016), "ICT Development Index 2016", ITU's website, accessed 1 December 2016, http://www.itu.int/net4/ITU-D/idi/2016/#idi2016countrycard-tab&PHL.

Lee Austin F. et al. (2012), "Predictiing hands-on child sexual offenses among possessors of internet child pornography", Psychology, Public Policy and Law, 18:644-72, 16 April 2012.

Mendoza, Ronal U., Olfindo, Rosechin, Maala, Camila Regina (2016), "Spatial disparities and poverty: The Case of three Provinces in the Philippines", Ateneo School of Government Working Paper Series, September 2016, accessed 3 December 2016, https://poseidon01.ssrn.com/delivery.php?

=882123066117005090064028006017012104017037064079033004076088091068091113087007124000036041017035040124044000112070007070003072038045044040053067030005096116125102056022083115124067121028117097085093004102118003 09.

Office of the President of the Philippines – Commission on Filipinos Abroad (n.d.), "Yearly Stock Estimation of Overseas Filipinos", accessed 1 December 2016, http://www.cfo.gov.ph/program-and-services/yearly-stock-estimation-of-overseas-filipinos.html.

Parents against child sexual exploitation (2015), "Keeping it together A parent's guide to coping with child sexual exploitation', February 2015, accessed 16 January 2017, http://paceuk.info/wp-content/uploads/Keeping-it-together-PDF.pdf.

Philippine Statistics Authority (2016), "Poverty incidence among Filipinos registered at 26.3 %, as of first semester of 2015 – PSA", 18 March 2016, accessed 2 November 2016, https://psa.gov.ph/content/poverty-incidence-among-filipinos-registered-263-first-semester-2015-psa.

Republic of the Philippines (1930), "An act revising the penal code and other penal laws (The Revised Penal Code)", Act No. 3815, 8 December 1930, Article 335 "Rape and Acts of Lasciviousness".

Republic of the Philippines (1992), "An act providing for stronger deterrence and special protection against child abuse, exploitation and discrimination, and for other purposes", Republic Act No. 7610, 17 June 1992.

Republic of the Philippines (2009), "An act defining the crime of child pornography, prescribing penalties therefor and for other purposes (Anti- Child Pornography Act of 2009)", Republic Act No. 9775.

Republic of the Philippines (2012), "An act defining cybercrime, providing for the prevention, investigation, suppression and the imposition of penalties therefor and for other purposes (Cybercrime Prevention Act of 2012)", Republic Act No. 10175.

Terre des Hommes (2013), "Webcam child sex tourism. Becoming Sweetie: A novel approach to stopping the global rise of Webcam Child Sex Tourism", 4 November 2011, accessed 2 November 2016, https://www.terredeshommes.nl/sites/tdh/files/uploads/research_report.pdf.

Terre des Hommes (n.d.), " WCST FAQ – WCST as a phenomenon", accessed 17 November 2016, http://www.terredeshommes.org/wp-content/uploads/2013/11/FAQ-English.pdf.

TheUKdatabase (n.d.), "Tech-savy paedophiles drive market for web-streamed child sex abuse", UK Database Online Sex Offenders Register, accessed 23 November 2016, https://theukdatabase.com/safety-tips-for-parents-children/tech-savvy-paedophiles-drive-market-for-web-streamed-child-sex-abuse/.

UN General Assembly (1989), "Convention on the Rights of the Child" (hereinafter CRC), Res. 44/25 of 20 November 1989, entered into force on 2nd September 1990, article 3 (2).

UN General Assembly (2000), "Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography" (hereinafter OPSC), A/RES/54/263, 25 May 2000, entered into force on 18 January 2002, Article 3 (1.a.i).

UNDP (2015), "Human Development Report 2015 – Work for Human Development", New York: UNDP, 229, accessed 7 December 2016, http://hdr.undp.org/sites/default/files/2015_human_development_report_1.pdf.

UNDP, "Frequently Asked Questions: Multidimensional Poverty Index (MPI)", accessed 7 December 2016, http://hdr.undp.org/en/faq-page/multidimensional-poverty-index-mpi#t295n2429.

UNICEF (2015), "Legal Protection from Violence Analysis of Domestic Laws Related to Violence against Children in ASEAN Member States", Bangkok: UNICEF EAPRO, accessed 17 January 2017, https://www.unicef.org/eapro/ASEAN_VAC(1).pdf.

1 July 2013, accessed 17 January 2017, http://www.refworld.org/docid/4538834f0.html.

UNICEF (2016), "Child Protection in the Digital Era. National responses to online child sexual abuse and abuse in ASEAN Member States", Bangkok: UNICEF EAPRO, 15, accessed 30 November 2016, https://www.unicef.org/eapro/Child_Protection_in_the_Digital_Age.pdf.

United Nations Treaty Collection (n.d.), "Status of treaties: Convention on the Rights of the Child", accessed 3 December 2016, https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-11&chapter=4&clang=_en.

United Nations Treaty Collection (n.d.), "Status of treaties: OPSC", accessed 3 December 2016, https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-11&chapter=4&clang=_en.

United Nations Treaty Collection, "Glossary of terms relating to treaty actions", accessed 25 November 2016, https://treaties.un.org/pages/Overview. aspx?path=overview/glossary/page1_en.xml#accession.

Western Union (n.d.), "Find Locations", Western Union's website, accessed 8 December 2016, https://locations.westernunion.com/search/philippines/ncr/manila?page=81&q=country%3APH%3Bcity%3AManila.

Wong, May (2016), "Myanmar's citizens look to English language to bring better prospects", Channel NewsAsia, 22 February 2016, accessed 17 January 2017, http://www.channelnewsasia.com/news/asiapacific/myanmar-s-citizens-look/2537670.html.

AUTHOR BIOGRAPHIES

Yvonne Nouwen

Yvonne Nouwen is the Capacity Building Officer at ECPAT International working to develop and provide training, workshops and various resources to increase awareness and knowledge about the issue of online child sexual exploitation. She has an academic background in Cultural Anthropology (BSc) and International Development (MSc) and has about seven years of experience working in the field of online child sexual exploitation and child sexual exploitation in travel and tourism. She previously worked as a project manager with the Dutch National Police and was advisor to the Board of Management of the Virtual Global Taskforce, an international alliance of law enforcement agencies working together to prevent and deter online child abuse.

Alessia Altamura

Alessia Altamura has a Master's Degree in Human Rights and Development Cooperation. She started working for ECPAT Italy in 1999 as programme coordinator and project officer on various initiatives to prevent the sexual exploitation of children. In 2005 she moved to ECPAT International Secretariat in Bangkok to coordinate an anti-trafficking programme that was implemented in Ukraine, Costa Rica and Thailand. After working five years as Regional Associate for Europe, she now collaborates with ECPAT particularly on research, policy and advocacy. Her main area of expertise is trafficking of children for sexual purposes.

Andrea Varrella

Andrea Varrella obtained her Law Degree in 2014. She also has a Master's Degree in International Protection of Human Rights from La Sapienza University in Rome, where she wrote her dissertation on the eradication of child, early and forced marriages in the framework of the SDGs. She currently works at ECPAT International as the Research and Policy Associate.

ECPAT International

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

Tel: +66 (0) 215 3388
Fax: +66 (0) 215 8272
Email: info@ecpat.org
Website: www.ecpat.org