EU Online Child Safety: What does the literature say?

J e f f r e y N. D e M a r c o
J u l i a D a v i d s o n
A n t o n i a B i f u l c o
M i a S c a l l y
Centre for Abuse and Trauma Studies, School of Law, Middlesex University

C a r l y C h e e v e r s
Geary Institute, University College Dublin

A d r i a n o S c h i m m e n t i
Kore University of Enna, Italy

V i n c e n z o C a r e t t i
LUMSA University, Rome, Italy

A n g e l o P u c c i a
E l i s a C o r b a r i
FDE Institute of Criminology, Mantova, Italy

J a n n e k e S c h i l d e r
S t e f a n B o g a e r t s
Tilburg University, Tilburg, Netherlands

Abstract (english)

The purpose of this review is to introduce both the research and political context of the European Commission's ISEC Illegal Use of the Internet work programme and the EU Online Child Safety investigation. This includes examining the social, psychological and legal contexts of online crimes perpetrated against children, inclusive of a holistic engagement with the relevant policy, legislation and law enforcement procedures within the European Union. The primary aim of this study is to

1

explore the prevalence of online childhood sexual abuse (online CSA) including the production, distribution and collection of childhood indecent images, online grooming and elements of 'sexting' from the perspective of law enforcement and industry.

The study covers four European countries and their associated practices: UK, Netherlands, Italy and Ireland, all of which will provide a comparative perspective of cross-cultural procedures and processes in law enforcement, industry practice and victimisation. This paper will address a summary of the key findings from the scoping phase covering all elements of the criminal justice process. Specifically, key summaries and themes emerging from the literature consulted are presented and recommendations are made for progress and as indicators for the project as it develops.

Keywords: *Childhood Sexual Abuse, Collaboration, Industry, Online, Police.*

Abstract (italiano)

Lo scopo di questa revisione è quello di introdurre le policy e le ricerche sviluppate all'interno del programma della Commissione Europea ISEC sull'Uso Illegale di Internet, nonché i risultati dell'indagine sulla Sicurezza dei Bambini Online. Questo comprende l'esame dei contesti sociali, psicologici e legali di crimini online perpetrati contro i bambini, passando in rassegna le pertinenti procedure di policy, legislazione e applicazione di legge all'interno dell'Unione Europea. Lo scopo primario di questo studio è quello di esplorare la prevalenza della fenomenologia dell'abuso sessuale su minori online (CSA on-line) compresa la produzione, la distribuzione e la raccolta di immagini pornografiche infantili, grooming on-line e gli elementi di 'sexting', guardandole da punto di vista delle Forze di Polizia e dell'Industria di Internet.

Lo studio copre quattro Paesi europei e le loro pratiche: Regno Unito, Paesi Bassi, Italia e Irlanda, i quali forniranno una prospettiva comparativa delle procedure e dei processi interculturali in applicazione della legge, delle prassi del settore e della vittimizzazione. Questo articolo

affronterà una sintesi dei principali risultati della fase di *scoping* che affronta tutti gli elementi del sistema di giustizia penale dei Paesi coinvolti. In particolare, sono presentati alcuni sommari e temi chiave che emergono dalla letteratura consultata, con l'obiettivo di dare alcuni suggerimenti in base ai progressi della ricerca e agli indicatori sviluppati dal progetto.

Parole chiave*: Abusi Sessuali su Minori, Collaborazione, Industria, Online, Polizia.*

Introduction

Any discussion of child sexual abuse and neglect, regardless of whether it is perpetrated online or offline brings with it a complex and vague interface of moral, social and political sentiment (Adams et al, 1999). Understanding and appreciating the complexities that arise between agencies including but not limited to law enforcement, social work and health care is of critical importance when attempting to structure prevention and intervention means and methods. Given the nature of online offending this research also explores the role and practice of industry as key stakeholders. As the offences being discussed are linked to online behaviour and identity, it is essential to understand and learn, disseminate and critique the influence, and practice within online industries in dealing with, mediating and mitigating online sexual risks to minor users. Therefore understanding how industry, from Internet Service Providers (ISPs) to Social Networking Sites (SNSs), work independently in preventing online offending, but also in collaboration with third sector organisations, government and policing is central to the entire study.

The Internet is an increasingly pervasive phenomenon. Nearly three billion people or alternatively almost 40% of the world's current population, are now online (ITU, 2015). Whilst the Internet offers abundant opportunities for education, networking and communication as an information superhighway, it can also manifest risk, particularly regarding vulnerable populations such as young children. Essentially, with nearly 90% of the British non-adult population owning and interacting on at least one Information and Communication Technology (ICT) device, such as a mobile phone, tablet or gaming console, risks are going to increase (ITU, 2015). Through

3

online mediums and platforms, such as chat rooms and instant messaging that are easily accessible with any one of the above-mentioned devices, our children are more susceptible to violence, abuse and sexual solicitation, such as requesting one to perform or generate erotic acts through ICTs (Harvard Health, 2008).

Therefore, although the risks differ between medium, person and device, they are very real and need to be considered. For example, research would suggest that the psychological profile of young people visiting online chatrooms are likely to be more isolated, lonely and depressed, thus vulnerable to grooming and exploitation (Wolak et al, 2003; Ybarra & Mitchell, 2005; Munro, 2011;Webster et al, 2014).

Martellozzo (2012) states that reports from leading agencies such as police forces, the Home Office and Internet Watch Foundation (IWF), corroborated by internationally varied academic research demonstrates that male sex interest in children is more frequent than previously thought and is likely to be under-reported. Cyberspace through the Internet has provided new and covert pathways for sex offenders to express their attraction to children. Additionally it has been asserted that offenders may be increasingly move online given restricted 'real world' access to children (Byron, 2008). The anonymity offered through the Internet (Joinson, 2001) and related technological instruments has motivated and provided confidence to particular offenders in searching for images to satisfy their criminogenic needs.

Law enforcement is charged with the duty to 'serve and protect' society, and this is done through criminal justice processes and policing styles. When one includes cyberspace into the potential mediums to be covered by formal policing, difficulties arise: Issues with deployment; abilities and policing styles are immediately subjected to new norms. Initially, the police response to online childhood sexual abuse has been seen as reticent, belated and uneven (Gallagher et al, 2006). This is in part due to lack of experience and appreciation for the seriousness of the problem as outlined above. In addition the scale of these online abuse operations are heavily hampered by lack of resources and expertise, thus hindering fast, efficient and proportional responses (Marcum et al, 2010; Wells et al, 2007). Operations such as Cathedral and ORE have highlighted the absolute need for law enforcement to enhance knowledge and skills in this area. This can occur through encouraging systematic reviews of national and international legislation, sentencing guidelines and procedures (Williams, 2003; 2004).

At the time of writing, police have invested in resources, training, undercover operations and have increasingly been improving their responses (CEOP, 2007; Eneman, 2010). However law enforcement cannot be the sole source of response; educational programmes for children, parents, carers and society are needed—online child abuse can be reduced by sharing responsibilities (CEOP, 2012; ENASCO, 2010; 2013; NSPCC, 2013).

Terminology becomes problematic as an investigation reaches greater depth, where the context and construct of the victim is not immediately clear and where there are grey areas in legislation. What are the social characteristics of the child being exploited online by their parents for financial gain versus those being used to satisfy sexual paraphilic urges and desires? How does one differentiate between the child who has been groomed to share explicit photographs online by an unknown stranger, versus the fifteen year old couple that have decided to share photographs as an output of adolescent risk and impulsivity? These are important questions to consider when teasing apart the complexities of online crimes against children, as often the discourse is anti-criminological or psychological; more emphasis is placed on populist concepts of crime, media representations and industry values (Abilio and de Almeida Neto, 2011).

Often there are incongruent values when policing and industry strategize individually when setting out preventative and intervention methods in dealing with online crimes against Internet users, particularly where children and adolescents are involved. Whilst the police may see crime in particular online behaviours, the corporation or commercial entity may see violations to user's privacy, terms and conditions of membership.

The current ISEC Project exploring online child safety across European partners is thus critical in unravelling the rules and regulations applied by industry and policing across jurisdictional and political boundaries. An understanding of the investigative process and models of collaboration, communication and partnership are needed, as already noted, law enforcement is not equipped to tackle online child abuse independently without the co-operation of other key players.

This document provides an overview and scopes out the landscape discussing the above issues and features of the debate. Specifically, it intends to examine and summarise the breadth of information surrounding the issues with policing online CSA, differentiated industry practice in its prevention and

intervention; the collaborative arrangements and initiatives taken by police across the globe with industry partners and the difficulties in definition and over-protection when considering the rights, lives and freedom of both children but also online users.

Methodology

The initial process in acquiring relevant literature involved the construction of complex search strings to meet the aims and objectives of the study. As the study involved key intentions surrounding the collaboration between law enforcement, industry and an understanding of victims, offenders and the ambiguity of crimes perpetrated against children in a cyber-medium, the strings were kept general and all-inclusive. These included operations encompassing law enforcement, industry, third sector, politics, offending and victimisation; each was independently searched but also every permutation and combination was included of the various areas. A sample search string may be located at Appendix 1.

The research pursued two primary directions: Firstly, systematically selected searches were conducted in mainstream databases and academic pool sources for relevant studies and literature. These included high volume and all-inclusive e-databases such as PsycArticles and Web of Science. Secondly, to encapsulate the grey literature linked to third sector information and policy development, searches were conducted in mainstream political and institutional websites including the Ministry of Justice, Interpol and the Home Office. For a full list of databases and sites used, please see Appendix 2.

Multiple online and e-repository databases were searched. Initially after searching through the first four databases (PsycInfo and PsycArticles, Web of Science, Hein Online and Criminal Justice Abstracts) as well as term searches on Google Scholar, the remaining databases were excluded, as the density of information from the former proved extremely relevant and highly saturated. The volume of information and data collected was of such an immense quantity, consequently the Project Manager in discussion with the Project Director decided to cease further investigation, for fear of data and information dilution. In addition, issues associated with access to particular databases, and parameter restrictions unique to individual search engines required a dynamic inclusion/exclusion process for resource pools. The latter meant

6

that information at times was difficult to acquire for the review. Some databases would not permit the research team to export large quantities of information; nor would they allow the structured search strings to be used in their complete and final form. In order to be consistent and standard across searches, where this was not possible (with the exception of Google Scholar), databases were excluded. Partner countries followed similar procedures.

In terms of the grey literature, government and policy websites dedicated to youth justice and the prevention of abuse against children were selected as being of high priority. Whilst searching the selected grey literature databases, a different approach to source identification and selection needed to be applied, as the complex strings were poorly suited for these non-academic sources. Key words and terms were used that summarised each of the individual permutations and combinations of the strings were applied, such as the procedure with Google Scholar. This included using terms that were deemed encompassing of associated terminology drafted for the syntactical strings. Table 1.1 presents the key word searches used.

The search was also guided by a set of inclusion and exclusion criteria that were first drafted by the Middlesex University research team, but also agreed upon and amended through consultation with Project Partners and the Advisory Group. Originally, over 100,000 studies were returned throughout all the searches, across strings and databases. As already discussed, the volume of information being returned to the research team proved problematic to handle therefore certain eliminations were engaged with in an ad-hoc manner. Where over 2000 results were returned by any particular data base, these were capped at 2000 which were then included into ENDNOTE 7X (software used for data storage, record keeping and referencing standards), which were then analysed first on title relevance/inclusion, followed by abstract relevance/inclusion and thirdly through an analysis of the entire documents/sources material. The latter step involved the mass search for irrelevant terms (i.e. CAT/PET/MRI/FMRI scan; diabetes; obesity; tobacco; gambling; cancer; melanoma). The final step involved a formal 'inter-rater' reliability check with the principal investigator, project manager and researchers where a selection of titles and abstracts were shared and included based on expertise.

Overall, more than 23,000 sources were highlighted from the search process, with a final number of 1038 documents

included in the analysis and discussion below. The following sections provide summaries of the literature searches deemed relevant to the study and policing of online CSA, and emerging themes and concepts are discussed.

Law and legislation

There are marked difficulties in the harmonisation and standardisation of laws dealing with online CSA at the local, national and international level. A range of legally binding laws interacts with non-binding policy and grey literature. As an over-arching foundation, the UN Convention on the Rights of the Child (UNCRC) provides a baseline definition for all citizens across geo-political boundaries under the age of 18 to be considered and treated as minors. The convention urges signatories to abide by this definition when considering all acts of exploitation, including those of a sexual nature and in the realm of cyberspace. This should, in the first instance, assist with the standardisation of laws and a joint-societal response.

In Europe, the European Union has enacted the Lanzarote Convention, which assists with bringing multiple members states to a general consensus in policing online crimes against children. The 2013 EU Directive is important in ensuring that all criminal justice authorities across the vastly different countries are able to work within some semblance of a framework whilst protecting young people.

Specifically in England and Wales, the implementation of a series of legal acts which cover a range of crimes perpetrated online against children, with the Sexual Offences Act 2003 central. This assists with a joint response in dealing across the real and virtual world and ensuring that all forms of online victimisation and anti-social acts are represented through the legal pathways. Other European partners are following similar provisions in an attempt to ensure common processes and procedures across the Union. Iterating the utility of the 2013 EU Directive, change and the line-up of similar services across international boundaries, at least in Europe, is becoming more of a reality. From a more global perspective, the International Centre for Missing and Exploited Children has attempted to provide information across all INTERPOL member states regarding legislation and practice. This does assist with the provision of visible and transparent information in the first instance; but the threat remains one of a global nature, and will

8

continue to be challenged by cultural and geographical differences.

Policing

As with policy and legislation, national and international law enforcement agencies are crucial in leading the implementation of preventative and intervention provisions within and across jurisdiction. This can be made easier, as discussed in the previous section, by the establishment of harmonised and standard policy. Policing may primarily occur within two modalities: Reactive policing is often undertaken, whereby police forces, through their specialist leads or units, pursue leads and evidence provided by national or international organisations; Proactive policing can be used with officers posing as both 'like-minded' offenders and minors alike, but can be difficult. Critical to the success of police forces in dealing with online CSA is the development and use of multi-disciplinary and diverse policing, including non-police partnerships.

Regardless of the law, policy and police strategies, there are issues surrounding funding, resource availability and mental health support for the law enforcement representatives working in this area of crime prevention. Ensuring support and readiness across the policing hierarchy is key in determining law enforcements ability to adequately police Internet-related sexual exploitation.

Victimisation

Increased use and engagement with ICTs when coupled with youth impulsivity, development and risk-taking behaviour presents unique situations and safety concerns to users online. As already discussed in the previous two sections, once of the biggest difficulties in supporting, identifying and understanding victimisation in the area of online crimes are centred within the lack of consensus on definitions of online CSA which may lead to ambiguity when understanding victimisation.

There are a myriad of risk factors used in determining likelihood of victimisation such as gender, parental supervision of technology use, age and risk taking behaviour. Online sexual solicitation and grooming through social networking sites has

9

become increasingly concerning in recent years, with most studies reporting approximately 20% of minors experiencing this type of behaviour on the Internet. Posting indecent images online (i.e. sexting, revenge porn) may quickly blur the boundaries between victim and offender, and question the legitimacy of 'deserving' victims.

Education and awareness amongst vulnerable youth is improving, but more needs to be done in highlighting the dangers of online victimisation whilst promoting the positive use and engagement with the Internet

Offenders

Internet sex offenders are generally male, White, relatively young, highly educated, intelligent, employed, and have less prior criminal history. Offenders are often known by the victim, whether this is an acquaintance, a family friend or a teacher. Often, they are people that children rely and depend on.

Internet offenders typically experience problems with intimacy, emotional loneliness, low self-esteem, under-assertiveness, and empathy. These problems are related to personality impairments that are known to lead to difficulties in developing and maintaining relationships with others. Internet offenders may suffer from depression and/or various personality disorders, as well as other mental health issues. Offender typologies typically describe Internet offenders as those that collect images with no intent to commit contact offences, those that collect images and intend to contact offend, and those that seek to make profit from distribution and production of images. These typologies are not set in stone and there may be progression from one typology to another. When considering the criminal careers of sex offenders, especially the evolution of modus operandi and behaviour, progression from non-contact to contact offences is disputed; with low levels of recidivism for Internet offenders and a low percentage rate for those committing contact offences as a result of Internet-based contact.

Explanations for sex offending include the concept of the Internet enabling offenders to commit offences by providing a space where anonymity and vast amounts of material can be obtained freely and easily, the concept of cognitive distortions resulting in offenders not fully understanding that their actions are harmful or feeling entitled to engage in offending behaviour,

seeking solace from young people looking for relationships due to isolation and general theoretical positions detailing more societal causes for offending behaviour, e.g. the male need to reproduce and the power imbalance between males and females.

What is evident is that there is a need to develop and identify specific rehabilitation programmes for Internet sex offenders. Offenders typically state that sex offender registration hinders rehabilitation and it is argued that computer limitations set by courts infringe on the human rights of offenders. Constitutional rehabilitation and restriction limits should be identified and tested more efficiently.

Industry practice

There are a multitude of government and non-government agencies working to protect the public and facilitate communication between those that can remove child abuse material and those that are identifying such material. There is, however a certain amount of conflict of interests between organisations that are profit based and organisations based on law enforcement. This should be addressed in order to provide more efficient and collaborative services;

In the United Kingdom, the majority of UK based Internet Service Providers (ISPs) have introduced self-regulation and are passing information on to law enforcement agencies. Whilst more could be done in this area, it is mandatory for ISPs to report identified abuse material to the National Centre for Missing and Exploited Children (NCMEC). Whilst it is not mandatory for Social Networking Sites (SNSs) to report child abuse material to NCMEC, most do have safety procedures in place and guidelines on how to deal with and report abusive content. Many also have guidelines for law enforcement and work alongside law enforcement to ensure young people are safe online. However, much more can be done by SNSs to ensure this. For example, CEOP highlight the need for the ClickCEOP function to be made available in Windows Live Messenger, one of the most frequently used SNS for grooming.

Young people are increasingly being provided with the tools to identify abusive content online and protect themselves from this. Research has identified that whilst young people have a good knowledge base regarding this, they rarely put it into practice. Many organisations are now creating software that is accessible to young people e.g. mobile phone applications, in

11

order for young people to be able to easily report abusive contact or content, however evaluations of outcome or process are non-existent as of yet.

Collaborative practices

Parents, teachers and other authority figures in the formative development of children must work together, with input from industry and law enforcement to ensure our vulnerable youth are protected. Youth also need to be mobilised to use the tools available to them and ensure safe use of the Internet. The ISPs need to assist in blocking indecent images of child abuse online in order to make the job for law enforcement and the third sector more manageable. There is a call across EU states to make blocking and removal of these images mandatory by law, but with different jurisdictions and legal interpretations, this can prove difficult. In addition, 'Notice to Take Down' (NTD) prove equally problematic when dealing with indecent images, with a lack of collaborative partnerships leading to delays and disagreements. With the inclusion of an increasing number of private contractors with Internet and computer-based products, come issues surrounding accountability, profit and equity. Industry partners can be hesitant for partnership with law enforcement due to the stigmatisation associated with childhood sexual crimes, and the effect that could have on the image of the organisation. However, this review has highlighted good practice, including the use of software to help collect evidence of offending behaviour. More of this needs to take place.
A lack of standardised law and practice makes it very difficult to deal with offenders operating across various countries. It also makes it difficult for agencies operating in multiple locations and can have serious complications for law enforcement when trying to prevent abuse from occurring. Law enforcement need to be provided with the tools to be able to effectively do their job and an international approach needs to be taken in order to combat the serious and devastating effects of child abuse material and grooming offences;
Organisations such as CEOP and the IWF have good practice guidelines and models set in place and collaborate well with other agencies, however a lack of evaluation makes it difficult to assess exactly what impact this is having and whether this can be improved. Evaluations of best and poor practice are

needed in order for agencies to grow and learn and in order to foster good solid collaboration.

Conclusion

The safety of young people online is of paramount importance. As ICT use continues to proliferate in individuals' daily lives, and a more frequent and substantial presence in cyberspace becomes increasingly essential to participate in communities, these threats to our children will only increase. Although much of what is presented in this document focuses on the dangers, risks and negative aspects of the Internet, it is undeniable that it also provides many positive tools and improvements to our lives. Regardless, more needs to be done in understanding these unstoppable threats to youth and assist in forging safeguards whilst promoting their participation in a hyper-connected society.

The literature review presented here provides a clear picture of the complexities surrounding Computer Mediated Crimes Against Children, also known as Online CSA. From the legal frameworks defining illegal activities such as the Sexual Offences Act 2003 and the contribution of instruments such as the COPINE Scale in influencing sentencing guidelines and practices, the Internet's own definitional characteristics of accessibility, anonymity and invisibility highlight the difficulties in prevention, prosecution and conviction. Whilst the Internet had reduced the spatial elements of our world, this creates difficult truths for judicial systems both at home but also abroad. Not all legal frameworks are well-equipped for collaborative criminal justice investigations. Despite these problems, organisations such as NCMEC, Interpol, Europol and CEOP have all taken positive steps in reducing the friction caused by international cross-jurisdictional investigations.

Police on the front line of online CSA face their own difficulties. Law enforcement agencies often lack standard practices and basic training, and the necessary tools at their disposal to be effective in policing online CSA. Issues linked to resource availability when dealing with evidence presented in binary code and terabytes cause operational hardships to investigative officers; where simple capacity is the least of problems when considering the well-being and mental health of investigative officers constantly dealing with explicit material. Coupled with limited understanding of offender pathways and

13

trajectories, and definitional blurring in victimisation with the creation, distribution and collection of indecent images, many of the aforementioned issues lead to further problems with law enforcement and individual household's ability to control the problem. Popular sentiment points towards industry taking a more central role in prevention and intervention of online CSA.

Industry, as with law enforcement, has made progress in dealing with the sexual exploitation of minors online, but as with law enforcement, cannot act independently. The expertise and technological frameworks provided and structured by industry need to be understandable by law enforcement, and inform policing practice. It becomes evident that collaboration between government, industry, the third sector and law enforcement is the logical and appropriate move forward, where the various specialisations can interact in a complimentary fashion in protecting our youth online.

In summary, the primary issues surrounding our societal response to online CSA centre on:

1. Jurisdictions and incongruent legal frameworks
2. Lack of police communication, resources and standardisation
3. Problems with definitions of victims
4. Invisibility and anonymity of offenders
5. Poor understanding of the pathway from online to offline offending
6. Risky behaviour of youth versus developmental behaviour
7. Industry aims and objectives incongruent with those of law enforcement

The current ISEC 'Illegal Use of the Internet' project intends to through its elaborate methodology, respond to many of these above issues.

14

References

ABILIO, C., & DE ALMEIDA NETO, S. E. (2011) *Internet Sexual Offending: Overview of Potential Contributing Factors and Intervention Strategies.* Psychiatry, Psychology and Law, 168-181.

ADAMS, C., ASHWORTH, A., BLYTH, E., COOPER, H., EROOGA, M., FEATHERSTONE, B. ET AL. (1999). *Children, child abuse and child protection: placing children centrally.* John Wiley and Sons Ltd.

BYRON, T. (2008) *Byron Review: Children and New Technology.* London: Department for Children, Schools and Families, and the Department for Culture, Media and Sport.

CEOP. (2007) *Working in partnership – CEOP principles on reporting online child sexual exploitation.* London: Child Exploitation and Online Protection Centre.

CEOP. (2012) *Relationship management strategy.* London: Child Exploitation and Online Protection Centre.

ENASCO (2010) *The right click: An agenda for creating a safer and fairer online environment for every child.* Report drafted by ENASCO in conjunction with the European Union.

ENASCO (2013) *The next click: Moving towards a better and safer environment online for every child.* Report drafted by ENASCO in conjunction with the European Union.

ENEMAN, M. (2010) *Internet service provider (ISP) filtering of child-abusive material: A critical reflection of its effectiveness.* Journal of Sexual Aggression. Vol. 16, No. 2, pp. 223-235.

GALLAGHER, B., FRASER, C., CHRISTMANN, K., & HODGSON, B. (2006) *International and Internet child sexual abuse and exploitation.* Huddersfield: University of Huddersfield.

HARVARD HEALTH (2008) *Protecting children and teens from cyber-harm.* Cambridge, MA: Harvard Medical Health Letter, Harvard Medicine.

INTERNATIONAL TELECOMMUNICATIONS UNION (2015) *Statistics: Aggregate Data.* Accessed Online 11 March 2015

http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

JOINSON, A. N. (2001) *Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity.* European Journal of Social Psychology. Vol. 31, No. 2, pp. 177-192.

MARCUM, C. D., HIGGINS, G. E., FREIBURGER, T. L., & RICKETTS, M. L. (2010) *Policing possession of child pornography online: investigating the training and resources dedicated to the investigation of cybercrime.* International Journal of Police Science & Management. Vol. 12, No. 4, pp. 516-525.

MARTELLOZZO, E. (2012) *Policing and protecting children from on line child sexual abuse.* Accessed online 17 April 2014 http://estudiobandin.blogspot.co.uk/2012/11/policing-and-protecting-children-from.html.

MUNRO, E. R. (2011). *The protection of children online: A brief scoping review to identify vulnerable groups.* London: Department for Education.

NSPCC (2014) *Changing childhoods together: Annual reports and accounts 2013/2014.* Document drafted by NSPCC for yearly account of activities and provisions.

WEBSTER, S., DAVIDSON, J., & BIFULCO, A. (2014) *Online offending behaviour and child victimisation: new findings and policy.* London: Palgrave Macmillan.

WELLS, M., FINKELHOR, D., WOLAK, J., & MITCHELL, K. J. (2007) *Defining child pornography: Law enforcement dilemmas in investigations of Internet child pornography possession 1.* Police Practice and Research. Vol. 8, No. 3, pp. 269-282.

WILLIAMS, K. S. (2003) *Controlling Internet child Pornography and Protecting the Child.* Information & Communication and Technology Law. Vol. 12, No. 1, pp. 245-261.

WILLIAMS, K. S. (2004) *Child pornography law: Does it protect children?* Journal of Social Welfare and Family Law. Vol. 26, No. 3, pp. 245-261.

WOLAK, J., MITCHELL, K. J., & FINKELHOR, D. (2003) *Escaping or connecting? Characteristics of youth who form close online relationships.* Journal of Adolescence. Vol. 26, pp. 105–119.

YBARRA, M. L., & MITCHELL, K. J. (2005) *Exposure to Internet pornography among children and adolescents: A national survey.* Cyberpsychology & Behavior. Vol. 8, No. 5, pp. 473-486.

Appendix 1: Literature Search Strings

1.   (online OR technology OR Internet OR "social networking" OR "Computer Mediated Technology" OR "CMC" OR "Social media" OR "Social networking sites" OR "SNS" OR "Virtual platforms" OR "SMS" OR text OR "Facebook" OR "Twitter" OR "Google" OR "Instagram" OR "Snapchat" OR "Tumblr" OR "Tinder" OR "Pure" OR "Blendr" OR "4chan" OR "deviantART" OR "Reddit" OR "Imgur" OR "MySpace" OR "ask.fm" OR "xboxlive" OR Gam* OR Console OR "ICT" OR Software OR chat OR "mobile telephone" OR telephon* OR phon* OR "instant messaging") AND (child* OR youth OR "young people" OR girl* OR boy* OR adolescen* OR teen*) AND (groom* OR abus* OR "online solicitation" OR Image* OR "indecent images" OR "Image collection" OR "Image production" OR "Image distribution" OR "Cybersex" OR "Sexting" OR "trolling" OR "flaming" OR "cyberstalking" OR access* OR "child sexual abuse" OR solicit* OR offend*).

2.   (Offender OR perpetrator OR groomer) AND (online OR technology OR Internet OR "social networking" OR "Computer Mediated Technology" OR "CMC" OR "Social media" OR "Social networking sites" OR "SNS" OR "Virtual platforms" OR "SMS" OR text OR "Facebook" OR "Twitter" OR "Google" OR "Instagram" OR "Snapchat" OR "Tumblr" OR "Tinder" OR "Pure" OR "Blendr" OR "4chan" OR "deviantART" OR "Reddit" OR "Imgur" OR "MySpace" OR "ask.fm" OR "xboxlive" OR Gam* OR Console OR "ICT" OR Software OR chat OR "mobile telephone" OR telephon* OR phon* OR "instant messaging") AND (groom* OR abus* OR "online solicitation" OR Image* OR "indecent images" OR "Image collection" OR "Image production" OR "Image distribution" OR "Cybersex" OR "Sexting" OR "trolling" OR "flaming" OR "cyberstalking" OR access* OR "child sexual abuse" OR solicit* OR offend*).

3.   (typolog*) AND (child* OR youth OR "young people" OR girl* OR boy* OR adolescen* OR teen*) AND (victim* OR survivor* OR "victim-survivor") AND (online OR technology OR Internet OR "social networking" OR "Computer Mediated Technology" OR "CMC" OR "Social media" OR "Social networking sites" OR "SNS" OR "Virtual platforms" OR "SMS" OR text OR "Facebook" OR "Twitter" OR "Google" OR "Instagram" OR "Snapchat" OR "Tumblr" OR "Tinder" OR "Pure" OR "Blendr" OR "4chan" OR "deviantART" OR "Reddit" OR "Imgur" OR "MySpace" OR "ask.fm" OR

"xboxlive" OR Gam* OR Console OR "ICT" OR Software OR chat OR "mobile telephone" OR telephon* OR phon* OR "instant messaging") AND (groom* OR abus* OR "online solicitation" OR Image* OR "indecent images" OR "Image collection" OR "Image production" OR "Image distribution" OR "Cybersex" OR "Sexting" OR "trolling" OR "flaming" OR "cyberstalking" OR access* OR "child sexual abuse" OR solicit* OR offend*).

Appendix 2: Source material & Databases

Academic
1.   PsycInfo/PsycARTICLES
2.   Web of Science
3.   Academic Search Premier
4.   HeinOnline
5.   LexisNexis
6.   Criminal Justice Abstracts
7.   IBSS
8.   Google scholar
9.   Ethos

Grey
10.   RAND
11.   JRF
12.   Barnados
13.   NSPCC
14.   Google
15.   Home office and other gov websites (gov.uk, legislation.gov.uk, justice.gov.uk, MoJ-AS)
16.   NCJRS
17.   Research gate
18.   GreyNet
19.   CIAONet (for full text pdf's only)
20.   www.childcentre.info/robert/database/

Other countries
21.   Policy related websites from other countries