Enhancing Police and Industry Practice

EU Child Online Safety Project

Funded by the European Commission

Julia Davidson, Jeffrey DeMarco,
Antonia Bifulco, Stefan Bogaerts, Vincenzo Caretti,
Mary Aiken, Carly Cheevers, Elisa Corbari, Mia Scally,
Janneke Schilder, Adriano Schimmenti, Angelo Puccia

Middlesex University London

Acknowledgements

We would like to thank the following for their assistance with this research:

Hannah Broadbent and Will Gardner, Childnet;
Dr Graham Ritchie, The Office of the Children's Commissioner;
UK Council for Child Internet Safety Evidence Group members;
ISEC Advisory Board, including John Carr, Claire Lilley and John Brown (NSPCC), Patricia Cartes (Twitter), Mick Moran (Interpol), and Katarzyna Staciwa (Europol CyberCrime Centre);
Dr Karen Ciclitira (Psychology, Middlesex University) for her help throughout the project;
Conference participants and stakeholders Dave Miles, Annie Mullins, Cathal Delany (Europol) and Julian Milan Platero (Interpol);
Centre for Abuse and Trauma Studies (CATS) Advisory Group members: John Carr, Ron Giddens, Dr Richard Graham, Professor Paula Nicolson, Peter Spindler, Tink Palmer, Geraldine Thomas;
DCC Simon Bailey; Ellouise Long, Natasa Blagojevic-Stokic and Giulia Perasso for support from CATS.
Lastly, a special thank you to Mr. Ciaran Haughton from University College Dublin for his hard work over the duration of the project.

Contents

1.0 Executive Summary

This report draws together the findings from the European Child Online Safety Project which was funded by the European Commission ISEC fund. The project was led by Professor Julia Davidson Middlesex University, UK with partners from University of Tilburg, Netherlands; University of Kore, Enna, Italy; Cyberpsychology Research Centre, Royal College of Surgeons; and the Geary Institute, University College Dublin, Ireland; and FDE Institute of Criminology, Mantova, Italy.

The project sought to draw together the evidence base on online offender and victim behaviour including:

- online grooming;
- possession, collection and distribution of indecent child images;
- Identification of policing and industry best practice in prevention.

The project also sought to promote cooperation between law enforcement and industry in developing and disseminating good practice models in the area of online CSA. Through collaboration, this will ultimately assist practitioners and professionals:

- To develop effective prevention techniques;
- In early detection and deterrence;
- With the provision of valid and recent research.

The project had three primary and interdependent objectives:

1. Link project specific risk characteristics with other risk factors for grooming, like risk-taking and sexual orientation concerns;
2. Creation of victim typologies of cyber-grooming to assist with identification of vulnerable individuals and groups;
3. Development of 'Best Practice' guidelines for industry and law enforcement in the identification and prevention of online childhood sexual abuse.

Methods

The research design incorporated a range of strategies and data capturing modes in order to collect engage and utilise the information in as rich and as informative a manner as possible.

A **series of case studies** on industry practice were constructed to illuminate how organisations are dealing with the increased threat of online CSA but also exploring their multi-disciplinary partnerships with law enforcement and other agencies. This

data also provided a unique insight into the relationship between industry and law enforcement. The information was collected through informal, semi-structured interview and where possible, site visits. In total, 4 case studies were undertaken with: a social media site; a social networking site; a large media virtual community and an internet discussion forum. These were constructed using reflexive accounts and narrative coherence.

Each country conducted a **series of stakeholder interviews**. These were conducted with professionals and experts across all disciplines linked to the safeguarding and protection of children online. The interviews captured information from policing experts, industry representatives, academics associated with online behaviour and sexual abuse, politicians, civil servants and third sector organisations, amongst others. Each interview was then transcribed and input into NVivo 11 for organization and analysis, thematic analysis was used to analyse the data. Key topics from the interview schedule were used for the first level coding of the document, the analysis was divided into categorizations across 3 key areas: *Contemporary Practice; Governance, Policy and Legislation; and Partnership and Collaboration.* A 'pilot' analysis was run in which 10% of the documents were scrutinized by two of the researchers from Middlesex University. The analysis was then discussed and quality assured to provide a form of inter-rater reliability ensuring consistent coding criteria. Upon agreement of basic themes, the entire sample was thematically analysed, and then circulated to each partner country, providing additional levels of inter-rater reliability.

A **large scale police survey** aimed to explore current policing practice, standards, strengths and benefits in dealing with the varied nature of online CSA. The aim was to achieve a sample size of 2000 police officers (500 from each country) from a range of ranks, jurisdictions, departments and forces. The project endeavoured to receive information and 'scope' the knowledge base surrounding policing in general, and not just specifically geared towards specialist high tech crime units. In total, 1401 police officers from three countries (United Kingdom, the Netherlands, and Italy) completed the questionnaire. Individuals who did not consent (N= 21) were removed from the sample, reasons for not consenting are unknown. The survey was administered online via SurveyMonkey to professionals working within the police force. Folliwng the agglomeration and cleaning of the data set using SPSS 21.0, a range of descriptive and inferential statistics were applied. Further information on this may be found in the relevant seciton on policing.

The **retrospective young person survey** aimed to explore the demographics, lifestyle, offline behaviour, online behaviour and online negative sexual experiences amongst a cohort of young adults (18-25) responding to questions regarding their experiences between the ages of 12-16. The aim was to achieve a sample size of

1500 young people (500 from each country participating country: Ireland, UK and Italy) from a range of backgrounds. Following the agglomeration and cleaning of the data set using SPSS 21.0, a range of descriptive and inferential statistics were applied.

Italy, Ireland and the United Kingdom conducted a **series of depth-interviews with self-referred young adults** who had responded to the surveys in their respective countries. They were recruited through an open-ended question at the end of each survey, specifically asking whether they would be interested in participating in either a focus group or interview focusing on some of the questions posed within the survey. A total of 9 interviews were conducted in all. Questions surrounding their use of social media, ICT devices and online activities were all queried, whilst highlighting their individual negative experiences, both sexually and non-sexually. All interviews were transcribed, and a process of thematic analysis was applied in identifying common themes across the participants, but also as a tool in highlighting distinctive features of vulnerability and resilience in navigating the vast virtual world.

Key findings

The key findings from this research are as follows:

1. There are key challenges in investigating and prosecuting online child sexual abuse cases across jurisdictions given differing legal frameworks and legal definitions of child (age of consent to sexual relations differs across the EU);
2. Law enforcement regularly encounter online child abuse cases, this was most marked in the UK ;
3. Police officers from the UK encounter online grooming cases and indecent image collection cases in equal measure;
4. The vast majority of cases are reported to local police officers by phone in the UK (approximately half of which are reported to specialist units) and are made in person to a local police officer in Italy and the Netherlands;
5. More psychological support is required for police officers, with calls for mandatory counselling and external support to be provided and it must be more accessible to investigative officers;
6. There is a lack of police communication, resources, standardisation and adequate focused training;
7. Police and industry professionals often differ in aims, objectives and desired outcomes in terms of strategy, operations and prioritization when dealing with online CSA;
8. There is a 'temporal incongruence' in dealing with online CSA, where the development of children, ICT devices/platforms, legislative development/ ascension of policy is 'out of sync' with one another;
9. Uneven resource allocation is a reality in investigating online CSA as unequal capabilities between industry and police;
10. When done well, working partnerships 'work'. They are the way forward. Models and frameworks of good practice should be sought and standardized;
11. Prioritisation of intervention & prevention must be of a multi-disciplinary, public health approach in which all agents involved standardize their approaches, with clear and coherent primary aims and objectives;
12. The invisibility and anonymity of offenders particularly on the dark or hidden web poses considerable challenges for law enforcement and little specialist training is available on this area;
13. Those police officers who were often involved with online CSA cases who had received specific training, perceived themselves as excellently or at least adequately trained, and in most cases routinely explored online risks with child victims and investigated the online behaviours of offenders. Those who were not trained and had not been involved in investigations of this type of crime rarely routinely explore the online behaviours of victims and offenders. This might strongly limit their ability to detect and deal with online CSA. This group of officers also reported the most effective working relationships with other agencies;

14. The police would welcome increased collaboration with industry in the online CSA area including: Mentoring, joint training initiatives; industry points of contact; joint work or task groups and input to educational awareness initiatives;
15. There are some good examples of effective inter-agency practice but this varies at national and international level and there is no standardisation of practice;
16. Whilst the majority of young people had not experienced any negative behaviour online, some experienced sexual solicitation, with over half of participants from the UK being solicited online, the majority had been solicited by peers not adults;
17. Under half of young people across the three countries stated that they had sent explicit material to someone online, although the percentage of participants that engaged in the sending of explicit material varied by country with less than a quarter of young people from Italy engaging in such behaviours;
18. Young people from Italy were far more likely to seek support when they had received sexual solicitation than young people from Ireland and the UK. Less than half of young people from Ireland and the UK sought support, compared to over three quarters of young people from Italy. This may highlight cultural differences;
19. Boys were significantly more often harassed/threatened face to face than girls were. However, boys engaged in such behaviour significantly more often than girls. Boys significantly more often harassed/ threatened someone else online;
20. Through the inferential analysis of the young person retrospective data, four distinct profiles of behaviour emerged. These were the 'adapted adolescent', 'risk-taking aggressive adolescent', and a split between 'inquisitive sexual and 'inquisitive non-sexual';
21. The 'adapted adolescent' was the most well-rounded grouping with low levels of anti-social behaviour and risks;
22. The 'risk-taking aggressive' demonstrated anti-social acts and impulsivity in both the real and virtual world;
23. The 'inquisitive non-sexual' youth were most likely to have risk factors linked to online risky behaviour such as sharing information unsafely online; downloading illegal content; and accepting strangers as friends however had low levels of sexual requests made of them;
24. Inquisitive sexual' youth were most likely to have risk factors linked to online sexual risky behaviour and solicitation, and were most likely to be solicited by strangers online;
25. The vast majority of young people 'never' had to deal with sexually explicit online requests. However, a significant minority did receive such requests 'often' or 'sometimes', when they were between 12 and 16 years old. In general, girls were significantly more likely to be invited to engage in sexual behaviour on the internet than boys were;

26. With regards to industry safety practice some young people complained that safety procedures and report mechanisms were too complicated to follow and there were also a number of misconceptions about reporting inappropriate material which stopped individuals from acting;
27. Basic good industry safety practice includes :
    - New users limited in their ability to post information until they are more active members;
    - A team of trusted administrators and moderators with standard procedures in place to protect site's users;
    - Utilising automated systems in conjunction with human moderators to ensure coverage and protection of users;
    - Standardisation of procedures and thresholds constituting inappropriate and problematic content;
    - Site rules which reduce the risk of under 18s being inappropriately approached by an adult;
    - Site provides law enforcement with information on a user complaint or legal action;
    - Proactive approach to collaborate with other industry partners.
28. Good industry general practice includes:
    - An understanding of the criminal law and communication with its representatives;
    - internal policy in protecting users in a 'pre-crime' model and an appreciation and use of software and technology in assisting with prevention and in intervention;
29. Developing technologies bring dynamic risk therefore new strategies and innovative solutions are of paramount importance in safeguarding children's online world. Law enforcement and legislation must become more agile and remain ahead of the changes.

Recommendations

The key recommendations emerging from this research are as follows:

1. **Clear shared international definitions of online CSA – supported by an updated UNCRC which includes cyber abuse**;
2. **Policy, legislation and practice must become more responsive and able to rapidly adapt to an evolving cyberspace**;
3. **The development of systematic policing and industry collaboration;**
4. **Industry contributions in the form of: Mentoring of specialist police officers; named industry points of contact for police forces; joint industry and law enforcement task forces – which could include other agencies;**
5. **Industry contribution to law enforcement training;**
6. **The development of specialist training at a basic level for all rank and file officers and the enhancement of more advanced training for specialist officers.**

The ISEC study allowed us to develop some key points regarding best practice of policing CSA. Each of the points below should be considered as essential in effectively policing online CSA cases:

A. **Knowledge of Relevant National Legislation;**
B. **Knowledge of Relevant International Legislation**;
C. **Increased collaboration with third sector partners and non-profit organizations**;
D. **Collection of evidence from ICT devices in Potential Online CSA cases;**
E. **Improve collaborations with other professionals**;
F. **Always investigate online activities of child sexual offenders**;
G. **Always investigate the offline activities of online groomers and those who collect indecent images of children;**
H. **Use the network of collaborations.**

2.0 Introduction

The Centre for Abuse and Trauma Studies at Middlesex University have, for the last two years, led a consortium of European partners at Kore University of Enna, FDE Institute in Mantua, Royal College of Surgeons Ireland/University College Dublin and Tilburg University, with funding through the European Commission's ISEC (Prevention of and Fight Against Crime) initiative. Led by Professor Julia Davidson, the multidisciplinary team is comprised of experts in criminology, sociology and psychology.

This report provides an overview of the aims, objectives and outputs of the investigation, as well as providing critical new original information resulting from the collection, interpretation and dissemination of the data.

The project built upon the recent evidence on offender online behaviour surrounding online grooming and indecent child images, in order to identify policing and industry best practice in prevention. Secondly, it explored the nature of youth risk taking behaviour and victimisation to draw some investigative support in understanding the behaviour, vulnerabilities and resilience of those most likely to suffer from crimes of this nature. The findings presented throughout this report will promote cooperation between law enforcement and industry in developing and disseminating good practice models in this area of online childhood sexual abuse, thus advocating greater online safety for children and young people. Additionally, a better understanding of online victimisation in retrospect will assist law enforcement, industry and all related services dealing with the consequences of online sexual abuse.

2.1 Scope of the problems/issues

The Internet is an increasingly pervasive phenomenon. Approximately 2.9 billion people, i.e., almost 47% of the world's current population, are now online (ITU, 2016). 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. Through online mediums and techniques, such as chat rooms and instant messaging that are easily accessible with any one of the above-mentioned devices, children are more susceptible to violence, abuse and sexual solicitation (Harvard Health, 2008). Therefore, although the risks differ between medium, person and device, they are very real and need to be considered.

Earlier literature has characterised the police response to online childhood sexual abuse as reticent, belated and uneven (Gallagher, Fraser, Christmann, & Hodgson, 2006). This is in part attributed to lack of experience and appreciation for the seriousness of the problem. In addition the scale of online abuse operations have been heavily hampered by lack of resources and expertise, thus hindering fast, efficient and proportional response (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 the sharing of responsibility (CEOP, 2012; Houtepan et al., 2014; ENASCO, 2010; 2013; NSPCC, 2014).

It is clear that differing international terminology, and categorisation of offences in the online child sexual abuse area often result in problematic investigations and prosecutions, this coupled with , differing victim constructs and grey areas in legislation mean that cases are often complex and challenging. Cases can include the child being exploited online via webcam by their parents for financial gain versus those being used to satisfy sexual paraphilic urges and desires? Criminal justice must 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 populist discourse is focused on stereotypical concepts of crime, media representations and industry values (Abilio & de Almeida Neto, 2011).

Often there are inevitably 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 goal will be prevention, disruption and prosecution, the corporation or commercial entity will consider violations to user's privacy, terms and conditions of membership and impact upon company image. This research has for the first time attempted to explore ways in which law enforcement and industry might work together more effectively and consistently in the prevention of online child abuse.

2.2 Theoretical foundations

There are a multitude of criminological and psychological explanations that attempt to explain aspects pertinent to the nature of online CSA such as; globalization, behavioural disinhibition, temporal incongruence, and the digital divide occurring between youth and adults. The following sections will briefly explore these concepts.

Globalisation

The nature and expanse of the internet causes jurisdictional, political and legal complexities unprecedented in the prevention and protection of youth before. An offender can live in one jurisdiction governed by one set of rules (e.g. the age of consent) and the victim live in another country governed by a different set of rules. Online CSA occurs in a sphere where geo-political boundaries no longer operate. As a matter of jurisprudence, there is an issue of territorial jurisdiction, right and authority. If different laws govern the location of the victim and the location of the offender, police authorities are going to be expected to collaborate, but this is not often an easy feat as when the decision to pursue charges (and what type of charges) becomes transparent, global politics begin affecting the outcomes of these issues more and more.

The issue of globalization can also impact upon ability for people to meet and make friends. It has never been easier for an offender to find a victim, and equally for an offender to find other offenders. Research has indicated 'that most paedophiles are isolated individuals with little or no social contact with age mates' (Prendergast, 1991). However, the Internet provides some sexual predators with support groups. This peer support may allow these individuals to convince themselves that their behaviour is acceptable and does not injure the victims. Offenders can form what social psychology describes as in-group out-group behaviour; offenders consider their 'support group' as part of their in-group that understands them and empathises with their struggle. Others are considered part of the out-group and are different to them so would not understand their needs. The Internet may provide offenders with the ability to interact with others without the anxiety that McGrath and Casey (2002) claim internet offenders may experience, and equally to find other individuals who share their interests – allowing validation and a feeling of belonging where they may experience interpersonal difficulties in real life situations.

With young people that are victimized on the internet being highlighted as 'at risk' both online and offline, it is easy to see how this globalization effect can place them at further risk of harm. Offenders often groom vulnerable young people, and with the internet being accessible to most young people now, whether via their tablet,

desktops or mobile phones, it is clear that home is no longer a safe haven, but another place a vulnerable young person can be targeted by online offenders.

Behavioural disinhibition

The internet provides a level of anonymity and invisibility that are critical in understanding human behaviour and crime online. In cyberspace we are no longer governed, by the conditions of location or temporal order (Johnson, 2010). An element of behavioural disinhibition and disembodiment can occur that Suler (2004) has linked to the desensitization (the diminished emotional responsiveness to a negative/aversive stimulus after repeated exposure to it) process. Due to our inability to ground ourselves in the physical and time-oriented world, our behaviours are not regulated by historically regular elements of behaviour. In a sense, we have freedom from societal constraints (or at least, the sensation of this). Unfortunately, this freedom brings with it limitless risks, dangers and threats. Aspects of anonymity remove the rule-laden structure of society, and provide a medium for misbehaviour, risk and impulsivity. In fact, recent theoretical development in the field of CMC contend that online communications enable conversational actors to engage in selective self-presentation and partner idealization, so that partners in CMC base their perception of one another on the selectively presented information exchanged through online communications (Tidwell & Walther, 2002). In this way, anonymity and lack of face-to-face communication may lower the individuals' relational boundaries, self-consciousness, and behavioural inhibition. Offenders are aware that they can act as they normally would not for fear of being judged or caught, they can hide away by masking IP addresses and using proxy servers, they can use different names and interact with people they wouldn't normally interact with. This behavioural disinhibition is facilitated by the internet. It is not just offenders however that may take advantage of the nature of the internet and the anonymity it provides. Children and adolescents, both considered vulnerable age groups discussed throughout this paper, are more likely to act impulsively whilst in the disinhibited and seemingly anonymous medium of the Internet (Baumgartner et al., 2010; Livingstone & Smith, 2014).

Digital divide

Young people are typically labelled as 'digital natives' (Prensky, 2001). That means that they tend to be more savvy and knowledgeable about new technologies. Young people today are never really offline; there is no dichotomy of being online and offline. The growth of social networking sites, chatrooms and online presence has provided a platform that challenges all elements of contemporary privacy and surveillance, and offers a medium for communication and discourse never before seen. Young people are at the forefront of this and their knowledge far surpasses

that of most parents or teachers. There is a digital divide as such when it comes to youth and authority figures. There is currently considerable attention on research highlighting the lack of schools educational awareness work around online child sexual abuse. Heslip (2013) argues that this is due to a divide between teachers and students in terms of digital literacy and the ability of school counsellors and teachers to lead in a digital literacy curriculum. Public anxiety involving online risks is likely exponentially inflated due to numerous factors, including the rapid growth of the Internet and associated technologies, and the growing gap between online understanding and literacy between children (vulnerable) and their parents (safe guarders). Contemporary cybercrime, especially in the field of child abuse, redefines the seminal concept of 'the other' in criminological work; strangers are no longer considered simply people we have not met, as those we know through online mediums are 'known others' (Davidson & Martellozzo, 2012).

Equally, policing is affected by this digital divide. Young people are using platforms that are rapidly changing and evolving. By the time the police have received training on one platform, another has been created. Offenders are able to develop techniques and use evolving technology to commit crime with the knowledge that many police forces do not have the training and resources to be able to identify every possible way of offending online. 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 police expertise and resource availability. The backlog of evidence, cases and hierarchical priorities becomes another layer to already complex criminological and forensic psychological phenomena.

Temporal incongruence

With the rapid expansion of the internet and its exponential increase in availability and use by young people in daily life, it is clear that there are some trajectories that have become out of sync and unable to relate to each other in the way they should, despite running in parallel. With the internet creating a space for anonymous or unmonitored risky behaviour, children are considered to be particularly vulnerable online. As a result of normal developmental factors, e.g. impaired ability when it comes to decision-making as a result of frontal lobe development, children are expected to take more risks online (Walsh, 2011). The frontal lobe is also linked to inhibition and impulsivity (White, Moffitt et al., 1994) and the development process of establishing sexual identity and discovering ones individual sexual identity, from functionality, orientation and behaviour (Arnett, 1995). Developmentally, children are going to take more risks as they learn to make decisions, however the internet

provides its own dangers when considering risky behaviours. For example, activities such as sexting, which may be intended for one person but then shared further than the intended audience. Here we can immediately see the temporal incongruence between development, technology and policy. There is an element of miscomprehension when considering teenage involvement and engagement with sexting. Educators and policy analysts alike are unsure how to proceed when dealing with the phenomena. This is something that is quite unique, and coupled with adolescent sexual identity and orientation, clashes with authority and the proliferation of technologies that are directed towards our private lives (EACEA; Education, Audiovisual and Culture Executive Agency, 2009). Teachers, who spend a great deal of time with our children, have no idea how to deal with sexting and face the criticism of law enforcement, parents and children themselves for overly punitive measures (Carr, 2010).

With technology evolving, young people's knowledge of the internet is surpassing those of older generations, and policy somewhat unable to keep up, there is an argument for technology industries and policing collaboration. However this is somewhat incongruent in itself, simply due to the differing aims of industry and law enforcement. Fundamentally, the complexities and barricades to collaboration can be explained by considering the differing perspectives and aims of the different agencies involved. Economic Loss Prevention Theory (Shearing & Stenning, 1981; Shearing & Johnston, 2013) explains this incongruence, where it postulates that industry wants their tools and practices to be harmless in the perpetration of crime. That is, they want to offer a product that causes no harm, and leads to no problems. Their concern is not with the offender, victim or criminal justice process. On the contrary, they want to provide a safe product for their customers, and make a profit. The Criminal Justice System on the other hand wants to make society safe for all those individuals involved. Therefore it is concerned with all actors, agents and agencies within its jurisdiction and realm. It does not see the particular industry partner as an actual entity of harm creation, but as a vulnerable actor that must fall under the jurisdiction of their protectorate. It is clear to see the difficulties that arise when attempting to manoeuvre the already difficult period of development being experienced by young people with the freedom of the internet and rights of children and industry in this respect.

Online Child Sexual Abuse offending

Online crimes perpetrated against children are a complex set of serious offences committed on the Internet. Here, the report will briefly focus on explaining indecent images, grooming, and revenge porn, as considered in full elsewhere in the report.

Indecent Images

Indecent images involve the creation, distribution and collection of sexually explicit images and videos of minors. In general, an indecent image involves the depiction of a sexual or suggestive act of any person under the age of 16 (England and Wales law). This can come in a variety forms that, dependent upon the jurisdiction and research, may be categorised or rated according to severity (for example using the COPINE scale). The gradual recession of indecent images of children into deeper parts of the Internet poses huge challenges to both industry and criminal justice authorities alike. The National Centre for Missing and Exploited Children (NCMEC) reported through January 2015 that they have analysed more than 132 million images and videos depicting apparent online CAM through identification software (NCMEC, 2015).

Grooming

Grooming is the process of an individual initiating online contact with minors, with the intention of commencing a sexual relationship involving both online and potentially physical, direct sexual intercourse via offline interaction. This process often involves the perpetrator garnering friendship, trust and understanding through conversation with the young person, with the intention of pursuing offline sexual contact (Davidson & Gottschalk, 2010). Whittle and colleagues (2014) found participants who had been sexually abused online and/or offline had a range of grooming experiences including manipulation, deception, regular/intense contact, secrecy, sexualisation, kindness and flattery, erratic temperament and nastiness and simultaneous grooming of those close to victim. The findings were similar to themes identified by other literature in this area. These tactics are likely to make the victims feel familiarity, love, trust, a boosting of confidence, emotional support, excitement but also a lack of control, confusion, reliance on the offender and distancing from family members.

Revenge porn

Revenge porn, defined by a Home Office fact sheet detailing the new crime in England and Wales (MoJ; Ministry of Justice, 2015), is 'the sharing of private, sexual materials, either photos or videos, of another person without their consent and with the purpose of causing embarrassment or distress.' One example of this can be through peer victimization such as sexting (sending nude, partially nude or sexually explicit photographs and/or videos, or text via an ICT medium, such as mobile telephone, to another individual). A young person sending an image to a friend or boyfriend/girlfriend may experience the problem widening further when peers take it upon themselves to share these images further than intended viewing and without consent. This can have damaging consequences, with some young people going on

to take their lives as a result of the bullying and harassment received as a result of peers sharing their images. The sharing of these images beyond their intended viewing without consent, and with the intention to cause distress or embarrassment would therefore be considered revenge porn.

2.2 Legislative and policy context

The law is trying to catch up with what is an ever changing and developing phenomenon. For example, in the UK the law now includes grooming (Sexual Offences Act 2003 England and Wales- add NI and Scotland). In 2006, the International Centre for Exploited and Missing Children (ICMEC) produced a report on the legislation within the 184 Interpol member countries with concerning results. Of these 184 members, just over half had no legislation specifically addressing child pornography, and 1/5 did not criminalise possession, regardless of intent to distribute (ICMEC, 2006). The subjective nature of the investigation, assessment and application of the law thus becomes evidently complex and difficulty.

The above should illustrate the legislative complexity of online childhood sexual abuse, characterised by a lack of international agreement regarding the legal definition of child and regarding what constitutes an online sexual offence against a child. Factors such as age of child in different countries and definitions of laws (i.e. only two countries specifically criminalise internet grooming – England and Wales, and Norway) have caused considerable problems in applying and adhering to a due process system of justice (Davidson et al., 2011). The introduction of the EU Directive (ref) in 2011 (enforced in 2013) has forced member states to criminalise online grooming and child indecent image production, distribution and collection. However the implementation of this directive at national level has been patchy (Carr, 2014). This is discussed in more detail below.

The UNCRC

The UNCRC provides a raft of cultural, socio-economic and political rights, underwritten by a covenant that ensures that the child's best interest is the primary consideration for policy. All countries have now ratified the UNCRC with the exception of the USA and Somalia. The UNCRC is clear regarding the legal definition of *child*, including any youth under the age of 18, but there is great variation across European jurisdictions and internationally. The UNCRC also contains important general principles that should be taken into account throughout all relevant legislation and measures, including the principle that the child's best interests should be taken into account in actions that affect them.

The European Union

Article 23 of the Lanzarote Convention states that, in the prevention and intervention of the solicitation of children for sexual purposes:

> *'…each party shall take the necessary legislative or other measures to criminalise the intentional proposal, through[ICTs], of an adult to meet a child who has not reached the age set in application of [article 18, paragraph 2], for the purpose of committing any of the offences established in accordance with [article 18, paragraph 1(a)], against him or her, where this proposal has been followed by material acts leading to such a meeting…]*

Article 18 from the **Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse** stipulates protecting minors from sexual abuse/assault through coercion and in accordance with national legislation. This was established through the real world consequences of sexual abuse cases with minors following online encounters (Webster, Davidson, Bifulco et al., 2012).

In relation to standard practice across European countries, Luxemburg is seen to have legislated and implemented practice that goes beyond what the Lazarote Committee suggests; specifically, the proposal of meeting a child is considered a criminal offence (Carr, 2014), however in England and Wales the Serious Crime Act 2015 introduces a new offence of sexual communication with a child. The new offence criminalises adults (a person aged 18 years or over) who communicate with a child under 16 (who the adult does not reasonably believe to be 16 or over), if the communication is sexual or if it is intended to elicit from the child a communication which is sexual. The offence applies only where the defendant can be shown to have acted for the purpose of obtaining sexual gratification.

Although strides have been made with the attempt to standardise practice and intervention/prevention, challenges still exist. In Carr's research forty six countries were approached, with a 63% response rate; of those countries indicating that there was protocol in dealing with these issues, 28% noted that they did not meet the terms of Article 23—these included Belgium, Romani, Portugal and Lithuania (Carr, 2014). There is clearly a long way to go in terms of the implementation.

Furthermore, Article 23 treaty of Lanzarote (CETS No. 201):

> *'…parties shall take the necessary legislative means to criminalise and prevent the intentional proposal through ICTs of adults to meet children…'*

This provides a very minimalist rule, and countries as well as signatories are expected to take on more strict legislation where and when necessary. Although this

is a European directive, it crosses international boundaries and can highlight some of the issues stretching across political boundaries.

The above can become problematic when local law and jurisdictional issues become entangled in an on-going investigation. The age of consent differs from country to country, due to the disparity of European legislation; this presents difficulties in investigating and prosecuting cases across jurisdictions. A brief summary of relevant legislation across the participating countries can be found in the literature review (DeMarco, Davidson, Scally & Long, 2015).

What is clear from the international and European legislation and policy is that there are marked difficulties in the harmonisation and standardisation of laws dealing with online CSA. Although the UNCRC defines children as under the age of 18 across geo-political boundaries, and urges all members' states to adhere to this definition when considering online sexual exploitation against children, this can be difficult with differing age of consent legislation which reflects different cultures and historical contexts. The EU has enacted the Lanzarote Convention, which assists with bringing multiple members states to a general consensus in policing online crimes against children;

- England and Wales have implemented a legislative framework which covers a range of crimes perpetrated online against children;
- Other European partners are following suit in an attempt to ensure common practice across the Union;
- ICMEC has attempted to provide information across all INTERPOL member states regarding legislation and practice, but international practice varies enormously.

2.3 Research Aims and objectives

The project sought to draw together the evidence base on online offender and victim behaviour including:

- Online grooming;
- Possession, collection and distribution of indecent child images;
- Identification of policing and industry best practice in prevention.

The project also sought as already discussed to promote cooperation between law enforcement and industry in developing and disseminating good practice models in the area of online CSA. Through collaboration, this will ultimately assist practitioners and professionals:

- To develop effective prevention techniques;
- In early detection and deterrence;
- With the provision of valid and recent research.

The project had three primary and interdependent objectives:

1. Link project specific risk characteristics with other risk factors for grooming, like risk-taking and sexual orientation concerns;

2. Creation of victim typologies of cyber-grooming to assist with identification of vulnerable individuals and groups;

3. Development of 'Best Practice' guidelines for industry and law enforcement in the identification and prevention of online childhood sexual abuse.

In order to meet the project objectives, the organisation of the investigation involved a set of distinct work packages with a range of quantitative and qualitative methodologies used, as well as varied dissemination strategies. Although distinct in their set-up and outputs, all were linked. This commenced with a scoping phase included a range of literature surrounding offending, victimisation, policing and legislation across the partner countries and more generally from the international annals. This was discussed above. In conjunction with the search of the literature, a series of in-depth stakeholder interviews were conducted to investigate differing methods, practices and priorities of institutions in dealing with online childhood sexual exploitation. Additionally, case studies of 'best practice' are presented as an illustration of current examples within industry partners of combatting and preventing online CSE. A large scale police survey was administered across countries to investigate police process and practice in the field of online child abuse.

The second phase of the study shifted its focus to victimisation, and online behaviours. This included the development of a retrospective survey (examining adolescent behaviour with a cohort of young adults) and associated depth interviews with self-referred victims of online sexual abuse. The aim was to highlight particular typologies and profiles of youth behaviour to assist with a range of stakeholders in understanding and preventing online sexual abuse.

2.4 Research design and methodology

The research design incorporated a range of strategies and data capturing modes in order to collect engage and utilise the information in as rich and as informative a manner as possible. Within the parameters of mixed-methods, triangulation is a

research philosophy where it is believed that applying more than one methodology across variations of a projects aims and objectives provides as critical assessment of the information present. It permits research teams to consider the information at a range of levels, and serves to fill gaps in the findings from one stream with those of another. Although the research presented within this report is not strict in its adherence to triangulation, the various methods applied within the different streams should provide an interesting perspective on the outputs emerging from the various strands. In the following section, elements of the methods applied within each layer of work are described.

Industry case studies

A series of case studies on industry practice were constructed to illuminate how organisations are dealing with the increased threat of online CSA but also exploring their multi-disciplinary partnerships with law enforcement and other agencies. The case studies provide a glimpse into the on-going practices of commercial organisations in dealing with the threats posed by online CSA and an increased adolescent and child demographic populating virtual communities, social networking sites and the general public cyberspace zone. Most importantly, this data also provided a unique insight into the relationship between industry and law enforcement.

The information about industry practice was collected through informal, semi-structured interview and when possible, site visits. This permitted key issues surrounding child protection and online CSA prevention to be discussed, whilst also providing the opportunity to see organisational practice first hand.

In total, 4 case studies were undertaken with: a social media site; a social networking site; a large media virtual community and an internet discussion forum.

Stakeholder interviews

Each country conducted a series of stakeholder interviews (n=10 in each, total N=40). These were conducted with professionals and experts across all disciplines linked to the safeguarding and protection of children online. The interviews were designed to capture information from policing experts, industry representatives, academics associated with online behaviour and sexual abuse, politicians, civil servants and third sector organisations, amongst others. More specifically, the interviews explored in greater detail precisely how online crimes related to children, such as grooming and indecent images are dealt with throughout the criminal justice process, from the point of discovery through to conviction and sentencing across the participating partner countries.

Each interview was then transcribed and input into NVivo 11 for organization and analysis, thematic analysis was used to analyse the data. Key topics from the interview schedule were used for the first level coding of the document, the analysis was divided into categorizations across 3 key areas: *Contemporary Practice; Governance, Policy and Legislation; and Partnership and Collaboration.* It should be noted that some of the discourse/text from participants was multi-labelled to provide more complex analysis and a glimpse into the inter-relationships between themes. We considered this approach to the analysis of qualitative data as the most appropriate to investigate the stakeholders' perspective and different point of views with respect to the investigated topic.

A 'pilot' analysis was run in which 10% of the documents were scrutinized by two of the researchers from Middlesex University. The analysis was then discussed and quality assured to provide a form of inter-rater reliability ensuring consistent coding criteria. Upon agreement of basic themes, the entire sample was thematically analysed, and then circulated to each partner country, providing additional levels of inter-rater reliability. This approach also allowed for the themes to evolve, merge and collapse. This measure was intended to enhance the validity of the research, in drawing upon the expertise of the multi-disciplinary team of researchers. These findings from the analysis of the stakeholder interviews can be found in subsequent sections of the report.

For an example of the stakeholder interview schedule, please see Appendix II.

Police survey

The survey aimed to explore current policing practice, standards, strengths and benefits in dealing with the varied nature of online CSA. The English version of the survey may be found in Appendix III.

The aim was to achieve a sample size of 2000 police officers (500 from each country) from a range of ranks, jurisdictions, departments and forces. The project endeavoured to receive information and 'scope' the knowledge base surrounding policing in general, and not just specifically geared towards specialist high tech crime units. Difficulties were faced regarding this component of the research across the consortium. Specifically it proved difficult to gain access to police forces in the Netherlands and Ireland. This issue was discussed with the EC and alternative methodological approaches were used to gather information. Methodologies have therefore been amended to respond to this unforeseeable issue.

Specifically, a mixed methods approach was used in Ireland as it was not possible to undertake questionnaires within the Irish police force. The mixed method approach

that was used to obtain data from Ireland entailed a mix of qualitative interviews exploring the survey themes and a small scoping study to explore the training and practice of police officers when interviewing child victims and child sex offenders (Specialist Interviewers); and the use of An Garda Síochána policy documents on the investigation of sexual crimes against children as a reference.

In total, 1401 police officers from three countries (United Kingdom, the Netherlands, and Italy) completed the questionnaire. Individuals who did not consent (N= 21) were removed from the sample, reasons for not consenting are unknown. The 1380 participants that remained in the sample included 679 police officers from the United Kingdom, 97 from the Netherlands and 602 respondents from Italy. Two people did not indicate the country where they were from. Please note that the number of participants differs by question due to missing data. The total N by question excludes the respondents that did not complete an answer for that particular question. Most people in the sample indicated that their rank was a police constable (N= 455; 33%) or detective constable (N= 193, 14%). See Table 4.1 for an overview of the sample characteristics by country. Results of the qualitative Irish data will be described in each section by involved subject.

The survey was administered online via SurveyMonkey (encrypted) to professionals working within the police force. Various forces were approached and requested to administer the link to police officers in their teams. Surveys were completed between September 2014 and February 2015.

Folliwng the agglomeration and cleaning of the data set using SPSS 21.0, a range of descriptive and inferential statistics were applied. Further information on this may be found in the relevant section on policing.

Young person survey

The retrospective young person survey aimed to explore the demographics, lifestyle, offline behaviour, online behaviour and online negative sexual experiences amongst a cohort of young adults (18-25) responding to questions regarding their experiences between the ages of 12-16. This age group was selected to facilitate data capture that may have been influenced by ethical protocols, but also to include a retrospective analysis of particular life experiences now that the participants were in their adult lives.

The English version of the survey may be found at Appendix VI.

The aim was to achieve a sample size of 1500 young people (500 from each country participating country: Ireland, UK and Italy) from a range of backgrounds.

As with the policing survey previously discussed, the survey was administered online via SurveyMonkey to youth across the countries. Surveys were completed between February 2015 and May 2016.

Folliwng the agglomeration and cleaning of the data set using SPSS 21.0, a range of descriptive and inferential statistics were applied. Further information on this may be found in the relevant seciton on young people.

Young person depth-interviews

As with the young person survey, a series of depth-interviews were conducted with self-referred young adults who had responded to the surveys in Italy, Ireland and the United Kingdom. They were recruited through an open-ended question at the end of each survey, specifically asking whether they would be interested in participating in either a focus group or interview focusing on some of the questions posed within the survey. Specifically, they were asked about their online behaviour in their adolescent years, with a focus on negative and risky experiences. A total of 9 interviews were conducted in all.

The interviews aimed to understand the perspective of the young adults about their lives as digital adolescents and what this meant in terms of both positive and negative experiences. Questions surrounding their use of social media, ICT devices and online activities were all queried, whilst highlighting their individual negative experiences, both sexually and non-sexually.

All interviews were transcribed, and a process of thematic analysis was applied in identifying common themes across the data, but also as a tool in highlighting distinctive features of vulnerability and resilience in navigating the virtual world. Details on the findings are available within the specific section in this report.

For an example of the young person interview schedule, please see Appendix V.

2.5 Ethics process

As the research was led by the Centre for Abuse and Trauma Studies at Middlesex University, all ethics processes were applied for through the lead organisation, with individual institutions also asked to adhere to their internal equivalents. This included a robust permission process whereby a thorough presentation of all tools, interview schedules and survey questions included, were presented to the University Ethics Board, with support material including information sheets; consent forms; debriefing sheets; sign-posting for support services in the case of discomfort; and an outline of how and when the research would be conducted, analysed and presented.

In adherence with British Society of Criminology and British Psychology Society standards for the research with human participants, the principals of anonymity and confidentiality were explained and where possible, adhered to for the participants across all work packages. In the case of interviews, pseudonyms were utilised to protect the identity of organisations and individuals.

All data was collected and stored under Data Protection Act, ensuring that only those with criminal background checks associated with the project would have access. These were also stored in the safety of the offices of the research team; either in locked cabinets or with password protected laptops and USB devices.

In the case of the young person interviews, a counselling psychologist was hired by each team involved with the collection of data under this work strand in the case of discomfort. Each team also provided information on support services particular to their geographical location. For a copy of the granted ethics permission forms, please see appendix VIIII.

2.6 Literature and policy review

The literature review and scoping exercise required a considerable amount of time and attention. More than 23,000 documents were identified and isolated through searches, through additional inclusion and exclusion criteria, this number was reduced to just over 1,000 for inclusion. An executive summary has been produced and can be found on the project website, highlighting the key themes and issues identified across:

- Policy and legislation
- Policing online childhood sexual abuse (CSA)
- Victimology of online CSA
- Offending related to online CSA
- Industry practice
- Collaborations

In summary, the key emerging issues from this review are as follows:

1. Challenges in investigating and prosecuting across jurisdictions and incongruent legal frameworks;
2. Lack of police communication, resources, standardisation and adequate focused training;
3. Problems in recognising and defining online CSA ;
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 and legal grey areas;
7. Incongruence between the aims and objectives of industry and law enforcement in the prevention and investigation of online CSA.

2.7 Summary and structure of report

This section provides a foundation for the research undertaken and presented in this report. It sets the scene with the policy and legislation at an international and EU level, highlighting some of the existent standards in place facilitating the investigation and prevention of online childhood sexual abuse, whilst also highlighting the key issues for police and society in tackling what is a perverse and widespread problem. In addition, the theoretical basis for the research was presented, demonstrating the global nature of the internet as both a medium for prevention and intervention, but also for criminality and harm.

Firstly, a presentation of industry case studies is made, highlighting elements of good and collaborative practice currently on-going across a range of technology organisations focusing upon networking and engagement. These will provide a 'snapshot' of current technological and industry practice in the protection and engagement of young people online.

This will be followed by an analysis of themes across the stakeholder interviews. Key commonalities between the internationally diverse and professionally varied group are highlighted, illustrating areas of good practice, concern and direction for the future in dealing with online sexual criminality and deviance.

The information from the cross-national police surveys follows, providing a theoretical grounding linked to the over-arching literature on police, criminality and cyberpsychology already discussed. This will then draw a picture of process, procedure, strengths and limitations across Italy, Netherlands and the UK. The utility of understanding how online crimes of a sexual nature are reported to the police, the quantity of reporting and contact police officers have, and the quality of their response and resources are discussed. Inferential analysis highlights the cluster and combination effects of training, contact with offence types and suggestions for future practice.

The young person surveys, victimisation and qualitative analysis will present for the first time a set of cyber-typologies. These typologies have been constructed through an understanding of young person risk, resilience, and protective factors, and looking at both real and virtual behaviours that the participants experienced over their adolescent formative years. The typologies are complimented by a thematic

analysis of young historical victims of online risks and sexual solicitation. These provide a rich additional layer in understanding what experience youth have had in the virtual world.

Recommendations, conclusions and future steps are described at the end of the document, with key findings integrated to offer suggestions for best practice and collaboration across police and industry. Recognition of vulnerabilities and risks, as presented from the young person quantitative and qualitative analysis are used to inform recommendations regarding practice and policy development.

3.0 Stakeholder and Industry practice

Prior to engaging in any discussion or presentation of findings linked to policing or young person perspectives, it is important to present a critical view of the practice and views of organisations dealing with technology and its risks. This section illustrates a series of good initiatives and practice in the technology sector of working across organisations and focusing on elements of safety, education and awareness whilst working proactively in combatting online childhood sexual abuse.

3.1 Positive narratives and practice in online child protection

A series of case studies on industry practice have been constructed to illustrate how organisations are dealing with the increased threat of online CSA but also exploring their multi-disciplinary partnerships with law enforcement and other agencies.

Case Study 1 – Importance of Trust with users and law enforcement

Discussion Board 1 (DB1) is a free online discussion website which was founded in 2000, with over half a million users post tens of thousands of time per day within 1,000 different, unique discussion strands. The majority of discussions on DB1 are available for anyone to view; however, individuals need to register as users in order to participate in discussions.

Private conversations on the site are limited to trusted, long time users

Generally, all posts are public meaning it is less likely that this platform will be utilised for inappropriate activity. There are some forums where members can have private conversations, but these private forums are limited and the privilege only extends to trusted members.

New users limited in ability to post information until they are more active members

New users are required to have made 50 posts and to have been active on the site for at least 10 days to be able to post images or hyperlinks. Until then, users can only post text. Prior to this, if an attempt is made to upload imagery or web links it will not work and be flagged to moderators.

A team of trusted administrators and moderators have standard procedures in place to protect the site's users

DB1 has approximately 628 moderators and 30 administrators who review content in order to keep any inappropriate material or discussions off the website. According to DB1, anything a member reports is examined by a human with a response actioned within minutes. If an incident involving child sexual abuse images should arise, the content is flagged and sent to an administrator or community manager, who will then contact law enforcement regarding the

issue. Should an individual post a child sexual abuse image, the post would be deleted, their account would be closed instantly and all data the DB1 has on the individual (all activity from the IP address for the previous 30 days) would be sent to law enforcement.

There are a number of site rules which reduce the risk of under 18s being inappropriately approached by an adult

Convicted sex offenders are banned from using the site. Users are also forbidden from soliciting *any* personal information from anyone under 18, and in general, from causing any harm to a minor on the site. The topic of pornography – images and discussions, is also forbidden on this site, meaning it is unlikely this site would be used as a place for an adult to use pornography to desensitise a minor to the topic of sex.

Site provides law enforcement with information on a user complaint or legal action

The way in which technology companies interpret Data Protection legislation impacts on the speed of law enforcement investigations. The DB1 believes that under national legislation it reserves the right to reveal any information it has on a user to law enforcement when necessary. This interpretation and practice means law enforcement investigations can move faster when dealing with investigations involving DB1 than they can when dealing with other companies.

Case Study 2 – Recognizing external expertise and competition

SMSx is a public social media website. As of early 2016, the site had 150 million unique users. The majority of SMSx's users are children under 18, and children need to be at least 13 years old to register on SMSx.

The SMS is heavily moderated by humans and automated systems

There are a large number of human moderators hired by the SMSx who review posts 24 hours a day, 7 days a week. The SMSx also uses automated moderation with a filtering programme which flags key words and language patterns linked to sexually explicit comments. As of the time of interview, all images posted to the site are dealt with proactively, with every image that is uploaded being checked by a human moderator.

The SMS has standard procedures to deal with inappropriate or problematic content

If posts or images are deemed inappropriate there are a number of actions moderators can take. This can include taking down the content, closing an offender's profile, and/or sending a report to law enforcement if such escalation is deemed necessary. SMSx also has the ability to block certain IP addresses for repeated violations of terms of service. If it is obvious that there

is immediate danger to a child or there is a threat to life, the issue is dealt with immediately.

The SMS collaborates with key organisations in an effort to deal more efficiently with child abuse images

The SMSx is a member of the Internet Watch Foundation (IWF) and has been negotiating a relationship with The National Center for Missing & Exploited Children (NCMEC). The SMSx is currently exploring whether it is possible to use the IWF's and NCMEC's lists of known child exploitation images in order to help remove as much child sexual abuse material as possible from their site. They are also currently working with the NCMEC on plans to send all child abuse images material to them so that the organisation can add unique images to their database.

The SMS has been guided by safety experts in order to protect and educate users

The SMSx's safety strategy has been developed by two world-class safety experts. It also has a safety advisory board and an online safety centre which includes tips and guidance for users.

The SMS has taken a proactive approach to collaborate with other industry

The SMSx has approached other social media companies with more experience in dealing with safety issues and law enforcement in order to help strengthen their knowledge of industry best practices.

The SMS takes a proactive approach to ensure effective collaboration with law enforcement

Once the SMSx set up its base in a new country, it sought guidance from other social media companies on how to build a relationship with law enforcement in said country. The SMSx then met with local law enforcement and agreed upon two operational elements to ensure effective collaboration. Firstly, a specially agreed template was developed to streamline the process of law enforcement requesting information from the site. Secondly, a single point of contact (SPOC) was established between the site and law enforcement so any information needing to be transferred is sent to the same contact. There is now personal contact between SMSx and law enforcement on a daily basis and these arrangements have had a positive impact on the exchange of information and relationship between the two.

Case Study 3 – Rise of training and onsite collaboration

SNS1 is an online public social networking and information platform in which individual profiles are able to engage in public discussions and statements ranging from conversations about mundane topics to political and ideological statements. In early 2016 there were approximately one quarter million users worldwide.

Working in partnership with law enforcement on site

Catering to a large international following, SNS1 spends a great deal of time working closely with the police training facilities in the UK. Unfortunately training demands exceeds the capacity of the organisation, and often many requests go unfilled. Documentation has been provided for police officers worldwide in dealing with policies and procedures with SNS1, to the extent that all languages are covered or available should a particular force or country be interested.

International standards and process

In addition, there are good partnerships within various countries where the police are trained and urged, through SNS1, to have an online presence easily accessible and reachable by vulnerable youth online. Applications for smartphones are consulted on with law enforcement and third sector organisations on a regular basis.

Proactive work in person and with technology

In terms of proactive prevention through SNS1, anti-grooming software is used in which particular risk factors (i.e., age difference of friends, multiple account holders) are identified and pursued. Basic linguistic analysis can also be applied. These types of initiatives are always changing and adapting to meet contemporary needs current threats.

Case Study 4 – Combination of efforts, resources and strategies

An internationally successful, multi-media, mass communication network which will be referred to as MMM engage in primary forms of prevention and intervention when dealing with online CSA: reactive and proactive.

Reactive prevention helps reduce volume going through criminal justice system

Reactive tools include reporting mechanisms enmeshed within the medium. This has different avenues for members of the public who feel at risk, harassed or harmed. There are additionally special, priority routes for police and law enforcement agencies to pursue if in need of critical information; and lastly

there are routes for third sector victim-oriented agencies.

Expert consultation very helpful to assist with understanding what they do well, and what they need assistance with

There is also a 'priority' expert list, in which MMM deals with organisations that have agreed to partnerships, facilitating open dialogue and data sharing. The partnerships are confidential and controlled by MMM under stringent conditions to prevent infiltration and these organisations are provided with specialised training from MMM to ensure the quick, efficient and optimal dissemination of information and evidence in suspect cases on online CSA. This assists all partners, as well as MMM, in sharing information throughout the investigative process. The partners serve as a 'port of call' for MMM and law enforcement.

Artificial Intelligence (AI) and Intelligence Amplification (IA)

The organisation appreciates the sheer volume of users, behaviours and risks that may present itself. With the global nature of their industry, and the difficulty in predicting and preventing the plethora of permutations and combinations of varying users interactions (both positive and negative), there is an increased reliance on both the use of technology that adapts and evolves as content changes; and through the evolving nature of the technology through moderator and employee input. In order to assist with 'policing' illicit content on their platform, MMM employs a series of software packages that adapt to individual user's reports and content; providing them with a dynamic 'trust' score. As the score changes based on their virtual activities, so too do their privileges and abilities online. In addition, the input of moderator involvement also allows this system to expand its remit, and apply new rules, considerations and parameters as time passes. This is seen as vastly important to not only allow the employees of MMM to do their jobs on a daily basis, but also in recognizing the importance and input of technology that learns and adapts; assisting in areas that could be problematic and may be prone to human error (or resource depletion).

Brief summary

An emerging picture of what can be done has been presented, from a non-law enforcement or legal perspective. A range of strategies linked to proactive and reactive 'policing' have been demonstrated as common amongst these organisations, where employees use strategies and initiatives to assist and ensure a safe space for their users. Partnerships with legal entities, such as national police are present, and an appreciation for expert input outside the realm of policing and technology is also acknowledged. Having direct lines of communication between relevant stakeholders, and organisations also assists with ensuring that the technology experts running these various companies have the capacity to protect

the privacy and rights of their users while assisting in preventing criminality and sexual exploitation. Finally, there is an appreciation for technology itself and what it can offer in assisting with intervention and prevention; as well as increasing the capacity of the human elements of engagement with these types of crime and criminal behaviour and victimisation.

Good practice can be identified in three distinct areas:

- ✓ **An understanding of the criminal law and communication with its representatives;**
- ✓ **Internal policy in protecting users in a 'pre-crime' model;**
- ✓ **Appreciation and use of software and technology in assisting with prevention and intervention**

3.2 Expert analysis: Thematic findings from stakeholder interviews

The information presented in this section was collected in the form of semi-structured interviews and a range of stakeholders involved with the intervention, prevention and protection of young people from online childhood sexual abuse across Europe participated (N=43). The stakeholders came from a range of organizational backgrounds including, but not limited to law enforcement; government and policy; Information and Communication Technologies industries (small and large businesses); behavioural science experts; educators; and academics.

These themes were structured through discussion, expertise and emerging from both previous work done by members of the project consortium, but also from the gaps in the literature surrounding internet safety, partnership and awareness. These themes, consistently identified across the interviews were: ***familial understanding and protection; risk; offender operation and invisibility; professional practice; difficulties; collaboration and partnership;*** and ***future practice***.

Familial understanding and protection

Stakeholders suggested that the concept of online risks and sexual victimisation are a relatively new threat to the family. Many parents and caregivers are unaware about the nature and extent of the problem, and the threats that young people face:

> *'…[online CSA] is a far deeper problem than [the public realise]…there is something deeply rooted in the culture of the internet that's allowing and reinforcing criminality…'*
>
> **(UK10, 2014)**

However, there are also those that are critical of technologies as a consequence of the media and stories linked to horrific experiences of grooming, revenge pornography and indecent image collections, distribution and production. Respondents stressed the need for good information and clarity, which were seen as necessary so adults can educate themselves on what threats their children are facing, whilst enabling and encouraging access to new technologies and information.

> *'…people [have a] tendency to be distrustful of new technology… 'technopanic', a kind of moral panic that occurs when something new is developed, and especially when it concerns children… [may lead to] implementing restrictions for children…'*
>
> **(Dutch3, 2015)**

The above quote illustrates a concern expressed by some respondents regarding the danger of moral panics and escalating fear in the context of the current movement towards increased use and engagement with technologies. The suggestion being that we must tread carefully and take precautions in teaching safety so as to not prevent access to the rich resource that the internet and associated technologies offer. Some respondents were critical of the lack of such awareness work:

> *'…there is the lack of tools and knowledge for this phenomenon among teachers and [parents] who could intercept signals and understand the needs of adolescents…'*
>
> **(Italy1, 2015)**

The problems in ensuring the family home is populated with 'safe' users often falls prey to the difficulty of defining victims in the complex and varied cases of online CSA. The victim of these crimes is often misunderstood, and as will be discussed in subsequent sections of this report, the range of organizational definitions and constructs in illustrating the 'ideal victim' causes additional layers of understanding and complexity by parents in monitoring, supervising and identifying whether or not their youth are being, or have been, the victim of online sexual abuse. In addition to these complexities are the cultural variations of definitions such as 'childhood', 'sexuality' and 'age of consent'. Providing parents, caregivers and teachers with a clear definition would be helpful in ensuring safety:

> *'…the worst thing that can happen around kids and digital technology is parents are panicked, schools are panicked and a number of the other agencies also [are unsure about the risks], and the discourse about the technology becomes more of a problem than what the technology might actually bring…'*
>
> **(UK11, 2014)**

'…[adolescents and parents] know [generally] the risks while they don't have a specific definition of each situation…'

(Italy4, 2014)

Therefore an element of concern is apparent in all stakeholder interviews. Respondents suggested that due to the nature of the indecent and sexual material, many of the youth do not necessarily appreciate the short and long term consequences of their behaviour.

'…[youth] are vulnerable in more than one way: they may have problems at home, social-emotional problems, perhaps they don't really understand how everything works, mental [health] may play a part…'

(Dutch3, 2015)

This in part may be due to the general nature of adolescent behaviour; where both risky behaviour and impulsivity are defining features of acting in particular ways. Exploring their own boundaries, identities and limits is important for later life stages, including the development of resilience, but does sadly still make them vulnerable to opportunistic perpetrators:

'…often adolescents actively contribute to these situations, due to their need for relation, risk, sexual experimentation and self-esteem.…'

(Italy4, 2015)

In addition, society must not engage in fear mongering, and allow youth to test their limits, and learn from their mistakes. Cyberspace and related technologies have changed the world, and our developmental processes in a manner that is not entirely clear—we want to ensure that young people are utilising the richness of technology at their fingertips, whilst being vigilant and aware, and knowing that should mistakes or risks be faced, there are ways in which these can be dealt with:

'…once you have reported to the police, the fear is that you can never get it out of the system and recover…'

(UK11, 2014)

Risk

Respondents expressed the general view that online child sexual abuse is more widespread than might be expected. It was suggested that the amount of illegal material circulating on the internet is vast and general awareness about this is low:

'…the extent to which people are engaging in behaviour that's entirely illegal is so prevalent and if you consider the amount of arrest and prosecutions that are pursued…relative to the number of people who are accessing image material there is clearly a problem…'

(Ireland3, 2015)

The stakeholder interview data across the countries suggests that online childhood sexual abuse material is a widespread problem, both in terms of accessibility and victimisation. Not only are there variations in content that conflict with cultural and societal norms and values depending on where in the world one is, there is also the difficulty of sheer volume. Cyberspace and the internet are vast constructs in a multi-media world. Regardless of policing the crimes being perpetrated against children online; or providing community care and support; or drafting legislation, it is suggested that the expansive and extensive nature of the phenome creates structural difficulties:

'…simply a huge amount of active teenagers who throw themselves at the internet, in front of the webcam, are making selfies and sending [material]. There is a vast amount of webcam-activity, of really young kids as well. I mean, we've seen 7- or 8-year olds doing the craziest things in front of a webcam…'

(Dutch4, 2015)

There is clearly wide scale recognition of online CSA and related material as a problem, but due to the nature, diversity and lack of standard practice in identifying and dealing with these crimes, there is an unfortunate strain on resources and consequently prevention. This will be further discussed in subsequent sections of this report.

'…preventive actions… could be implemented on the basis of a concrete analysis of the phenomenon, with the support of a [specific government unit]. Without [clarity], we grope around in the dark while the government will continue to finance different awareness campaigns…'

(Italy2, 2014)

The above is not necessarily symptomatic of political infrastructures across European and International organisations, but does echo the extent of the risk, and ambiguity in appropriately dealing with it at the macro-societal level.

Offender operation and invisibility

With cyberspace and the increasing world of the Internet of Things (IoT), our experience and understanding of offending behaviour has been challenged.

Cyberspace and anonymous communication networks, such as ToR (The Onion Router) provide an expansive environment for potential offenders to roam with little control over their actions and behaviours. Linked in with elements of online disinhibition such as anonymity and invisibility, stakeholders suggested that this causes difficulties for all interested parties in identifying offenders, protecting victims and providing safe and secure environments for learning and growth:

> *'…there is an increasing demand for knowledge from policemen and -women themselves, because there's still a lot of unknown with respect to online cases while they do come across such cases more and more often…'*

(Dutch6, 2015)

When including the relative ease with which perpetrators are able to operate whilst in the virtual world, the issues of legal jurisprudence, resource allocation and prioritisation of aims becomes even more complicated; as does the management and functionality of multi-stakeholder partnerships. Regardless of the lead entity in pursuing the offenders being police, industry or government, cyberspace causes difficulties for all involved. Making requests for information across organisational employment boundaries can often lead to differences in opinion and :

> *'…something that occurs a lot in Internet crime is the anonymity of the offenders… also IP-addresses that constantly change…often there are too many [offenders] hiding in cyberspace…this makes things difficult'*

(Dutch10, 2015)

As important as the concepts of understanding safety, victimisation, risk and offending are in order to provide an appropriate and effective service for protection, prevention and intervention, examples of operational practice, it was clear from stakeholder interviews that many difficulties exist in terms of collaboration and training.

Professional practice

Linked directly to the above concerns are the importance of speedy identification and prioritisation of issues, from a multitude of perspectives. The victimisation of young people online is about both the identification and awareness of the commission of a crime:

> *'…[partner] can act very quickly …[recently] there was a request from the police for a man sextorting a child on [SNS] who had been identified at 2300 Thursday evening. We made a report by 0800 on Friday and the man was arrested Friday PM…'*

(**UK12, 2014)**

Stakeholders suggested that it is also about the precedent being set as technologies evolve and move towards the larger multi-media world of the Internet of Things (IoT):

> *'…can certainly be improved [investigative process of dealing with online CSA] and that has to do with the capacity and quality, and also with the ever-changing [technological] environment, I just mentioned the digital world, containers and clouds, and further…'*

(Dutch7, 2015)

Another key issue raised was the human factor, including, repercussions, need and responsivity. Criminality is an inherent part of any society and although much of the research has focused upon prevention and intervention, we must also consider the importance of equipping users with safety tools they can easily use in making themselves less vulnerable and more resilient to online threat: ,

> *'…work in schools is very important---assist with children's resilience…their critical ability to exist and make decisions online. They need to be able to identify and recognise problems online. They need to be informed and educated that should something occur to them online, they need to speak to CHILDLINE, parents and teachers...'*

(UK8, 2014)

The above quotes demonstrate that not only is basic information and awareness critical in ensuring a safe, enriching and lively online footprint, but points to the potentially negative impact of moral panics upon young people and their parents. Through the use of overly negative narratives around young people's' online experience, we risk creating a reluctant, scared and anxious generation of users, who in turn may not benefit from the opportunity and resources that technology offer. Ensuring that youth are equipped with knowledge, and made aware of support mechanisms and networks, should ensure that 'mistakes' and errors in the digital sphere become manageable, and recoverable:

> *'…adults are quick to fear all sort of things, but I think that's not really helping children. So, from a positive viewpoint, teach them how to use the internet wisely and sensibly. Posting videos on YouTube for example, that's a creative way of using the internet, but someone may post unpleasant comments. How do you deal with that?'*

(Dutch3, 2015)

There are certain challenges facing law enforcement in their drive to be efficient and effective providers of process, justice and protection. As discussed before, the scope and scale of the problem is global and cyberspace is a difficult environment to

engage within for police work. Lack of communication, resources and standardisation are three key areas that, of no particular agents fault, can lead to issues in the ability to administer the law. Inconsistent jurisprudence fundamentally impact upon the capacity and capability for law enforcement to perform effectively in investigating online CSA. This includes issues around training, expertise and ability in efficiently and effectively dealing with crimes of a technological or computer-mediated nature:

> *'…that's the concern in terms of the numbers in the Computer Crime Unit, it's very difficult to get in Gardaí who are anyway qualified in computers, you need somebody who did a computer degree before they joined the job or something like that and there's a number of them in training but they obviously have to do a period of time.'*
>
> **(Ireland11, 2014)**

Not only are there feelings of inadequacy or lack of expertise, there is also a clear and fundamental problem around lack of resourcing:

> *'…one of the biggest problems is that the resources are simply not available in the area of policing and prevention—ACPO is aware that we cannot arrest ourselves out of this problem. Between 50,000-60,000 people viewing images on a daily basis—this is probably a conservative estimate…'*
>
> **(UK8, 2014)**

Stakeholder interviews suggested that the police and affiliated organizations understand the scale of the problem, but still feel overwhelmed and ill-equipped in dealing with it:

> *'…they may try to get us to take on cases but we are so overwhelmed that usually we just offer advice and that's all we can do.'*
>
> **(UK1, 2014)**

Law enforcement is well aware of the prevalence and difficulties in policing these matters, as have pointed to the importance of being equipped with the right tools to deal with the needs of the victims and their families. There may be a lack of awareness about the roles and expectations of various departments and agencies, which needs to be rectified in order to improve collaboration, service provision and investigative capabilities:

> *'…I think there needs to be a really clear outline of the boundaries of organizations' capabilities. Be they telecoms operators, be they over the top or internet service providers, or, um, or law enforcement. And how that's effective because you, you know, you have organisations who attract*

overlapping legal obligations because they operate in more than one country and law enforcement's hands are tied by virtue of the fact that their jurisdiction extends to one and being able to tease that out would be, would help people make a clearer decision in the future…'

(UK5, 2014)

Difficulties

There are a number of issues beyond some of those surrounding practice that cause further difficulties in the realm of prevention and intervention regarding online CSA. Specifically, there is a 'temporal incongruence' around three key factors: offenders use of technology (the move to the dark web for example); children and young people are ever changing use of technology and online behaviour; the online environment and the tools used. This is compounded and further complicated through developmental 'lifespans' of maturing children/adolescents; evolving ICT devices and platforms; and legislative development and ascension of policy and law and differing legislation across jurisdictions. Each of these factors operates on differing timescales and as a result they are all 'out of sync' with one another, thus contributing to difficulties and challenges for all agencies involved including the police, the third sector and industry in dealing with online CSA.

'…one obstacle that still remains is that all legislation, international and national, is lagging behind on how the world is changing. All of our legislation is not based on a digital world, which is simply faster and bigger than the hands-on world on which legislation is based...'

(Dutch4, 2014)

Technology, human development and legislation all function on differing times scales. Where technology is ever-changing, and biology and genetics have pre-determined progressive phases that they must surpass, legislation can be very temperamental and heavily influenced by socio-historical contexts. Ensuring that multiple stakeholders understand the dynamics of each timescale can ensure that various partners critically consider how to provide safety messages and protective services:

'…it would be good if every police force had a named point of contact with the big industry players. Someone they could seek advice from. Someone who is aware of changing policy and laws…

(UK1, 2014)

Stakeholders suggested that there can be uneven resource allocation when dealing with crime and justice across policing departments, forces and jurisdictions. In the UK, with the implementation of both the Crime and Disorder Reduction Act and Police and Crime Commissioners, increasing regional governance is being provided to meet locally-identified threats and problems. Additionally, the technology industries, regardless of their mandates, function on very different budgets, aims and objectives. Law enforcement finds it very difficult to keep up with the sheer volume of material that is being identified. This is strongly linked to another key theme surrounding the emotional, psychological and mental toll on investigative officers at all levels:

> *'…the actual resources that is to local police forces in terms of the forensic examination of evidence means that some forces have got back logs of about 12-18 months. Is it so surprising that they feel at times overwhelmed no it isn't.'*
>
> **(UK4, 2014)**

Stakeholders suggested that industry as previously discussed also does not work in a 'law and order' framework, their main concern may not necessarily be exploring the privacy settings, content and age of their users. They will of course adhere to the laws governing illegal and harmful content, but additionally may not necessarily be as attuned to the geo-politics of laws and illegal behaviour:

> *'Ensure the proper training of personnel receiving or processing such reports including training in the legal requirements of internal policy, the legislative threshold for child abuse material, being able to properly distinguish between inappropriate behaviour and illegal behaviour and categorise/describe these accordingly to Law Enforcement in their reports.'*
>
> **(Ireland10, 2014)**

On the contrary, law enforcement and related entities are constantly affected by government austerity measures, as well as public scrutiny and accountability. This causes difficulties in both attempting to investigate reported claims of online childhood sexual abuse, but also in adequately following through with the investigation of the evidence, and the associated links to the prosecution services across the countries involved. Often it is not a question of whether the legal entities wish to pursue a prosecution, but whether or not the information and evidence that they collect withstands the burden of proof in influencing juror decision-making:

'…is the phrase justice delayed is justice denied so therefore they won't go ahead with the prosecution because it's taking such a long time for the computers to be examined. And that's coming up quite a bit…'

(Ireland11, 2014)

Additionally, police often do not have the appropriate training (depending upon their rank, force and role) in dealing with a crime that can be reported at any time and via any source. We begin here to see the complexities of efficient partnership; multi-disciplinary productivity and inter-organizational communication breakdown, exacerbated by the scope, structure and ambiguity of online CSA crimes (in certain circumstances):

'…need to provide more resources to prevention services, for example to ensure proper and continuous training…give them tools to detected in due time signals of [children] being victims…'

(Italy3, 2014)

When considering any multi-disciplinary partnership, there is a need to ensure that various organizations, from a range of industrial, commercial and public backgrounds agree to terms, remits, aims and objectives. Where this is not strategically open and flexible in the first instance, difficulties may arise. Having these different aims and objectives, especially between police and industry can dictate strategy, operations and prioritization when dealing with online CSA:

'…incredibly difficult to get industry to the table and get them to act in a timely way and you'll see all sorts of debates now around preserving telecoms data and this whole argument of privacy versus security which actually is completely the wrong way of looking at things, it isn't a continuum, there isn't security at one end and privacy at the other. They're on different scales…'

(UK10, 2014)

In any partnerships, multiple disciplines will have a variety of expectations and modes of operation. It is not always an easy task to bring different agencies together. In theory, these cross-disciplinary partnerships are the most appropriate way forward. Sadly once inner programmes, agendas, deliverables and outputs begin to be overly clear, the comradery and functionality of the partnership can break down:

'…a lot of lone voices out there and some of them do great training for example with the police and stuff but the positions are disparate and they are generally informed by their own agenda…'

(Ireland3, 2014)

There needs to be central leadership, either through task forces appropriately led which operate under the guise of one agency, but bring the expertise of the multiple stakeholders together. As this is a crime in which children are being exploited, it is often believed that law enforcement should take the lead:

> *'…You can't do this [several] times over, it needs central co-ordination and what you don't want is proactive officers in all different forces doing their own thing targeting their own bits of the web, targeting individuals…'*
>
> **(UK10, 2014)**

However they must be equipped assisted and supported by expertise from the other areas in which they are not necessarily specially trained or contain the necessary knowledge and expertise to combat:

> *'…it would be good if every police force in the UK had a named point of contact with the big industry players. Someone they could seek advice from. Communication is key…'*
>
> **(UK1, 2014)**

Collaboration and partnership

Moving forward requires a consideration of the issues discussed, and as a consequence we require models and frameworks of good practice to be developed on the basis of sound empirical research and good practice experience. The research has highlighted key provisions and suggestions for improving work across geo-political boundaries; legal frameworks; and societal provisions. In order for any progress to be made in dealing with online CSA, a real joined up partnership needs to be visible, functional, effective and seen as legitimate:

> *'…I think the safer internet centres became legitimate when the European Commission said "we'd put money in and we network and this is the way that we want it to work"…So I would have something in legislation that says let there be a safer internet centre, let there be a multi-stakeholder coordinated body for…Child internet safety. And let everyone see that those are the recognised ways of doing things and get somebody behind them...'*
>
> **(UK11, 2014)**

Utilising individual organizational strengths, whilst acknowledging key weaknesses will provide an honest and respectable level of both ability and knowledge, which in turn may assist with a more structured and directed effort. Knowing exactly how and where the police need assistance; what more the corporations may do for ancillary

services; understanding the placement of NGO's and community groups within the realism of crime, deviance and victimisation in the context of online CSA can clarify roles and responsibilities:

> *'…[we need] police and companies to work together and joint training and joint events will encourage this. Information exchange mechanisms and frameworks should be put in place and if this is not possible in a self-regulation way then it should be legislated…'*
>
> **(Ireland12, 2015)**

Lastly, the participants were able to provide a range of recommendations of what collaboration, partnership and prevention will look like moving forward.

> *'…what's coming, what shape will the future take? They've given workshops at conventions as well. So we're combining the mediacoaches and policemen's expertise so they can help each other out. A lot of schools have an officer stationed in their community or assigned to the school…'*
>
> **(Dutch1, 2015)**

Although vague, these quotes show the urge for joint up services and non-traditional roles within protecting young people in a digital age; whilst acknowledging all the positives of cyberspace, understanding the need for awareness and resilience is of utmost importance and instilling youth with authority figures who are informed and aware will support their technological and normative development.

SUMMARY

Key stakeholders from across the participating countries were recruited from a range of disciplines. Through a thorough thematic analysis, elements of good practice in protecting youth online were identified; and the sign-posting of priorities for a range of individuals in the lives of developing youth: parents, teachers, and traditional law enforcement agencies. Understanding the ease at which offender's may operate and thus the information parents and young people need in order to navigate the virtual world are of critical importance. Collating examples of good practice in online protection from a range of organisations is useful for parents, police, young people and other industry partners as well. Learning 'what works' and differentiating good practice from that which is unclear or dated will assist all individuals in working together within a better and safer virtual community. It also equips young users with the knowledge that as they explore online, and anti-social or negative experiences present themselves, there are support services and programmes that can assist.

Finally, acknowledging that with technologies come dynamic risk, new strategies and innovative solutions are of paramount importance in safeguarding the online world; and structuring good, legitimate working partnerships between the various stakeholders; remembering the positive and beneficial aspects of the internet.

4.0 Policing

4.1 Context: Policing sex offences against minors in Cyberspace

Policing online CSA is a serious and fast developing field of interest for police all over Europe and internationally. The current project sought to explore how police forces in the United Kingdom, Italy, Ireland, and the Netherlands investigate and process these online offences in the context of EU and wider international legislation and policy. A questionnaire was developed and administered, which permitted us to capture information about police officers' knowledge, experience, and training in the field of online sexual abuse against minors in the United Kingdom, Italy, and the Netherlands. In Ireland, it was not feasible to conduct a survey due to access problems. Instead, a mixed-methods approach was used to provide the Irish perspective. This section provides the wider theoretical context of the environment in which police officers operate in Europe to combat online CSA , and explores the differences and similarities in policing online CSA in the United Kingdom, The Netherlands, Ireland, and Italy.

In Europe, Europol acts as the 'central European hub' (European Parliament of Justice, 2015, p. 32) in combatting cybercrime and inclusive of online CSA Europol is allowed to handle all serious crimes, including computer crimes, if the crime affects two or more member states. Information concerning these kinds of crimes are collected, stored, analysed, and exchanged (European Parliament of Justice, 2015). This facilitates better research and collaboration among EU countries in order to combat online CSA. As a more specialized cybercrime unit of Europol, the European Cybercrime Centre (EC3) was established in 2013. One of the areas in which EC3 acts is that of online child sexual exploitation wherein EC3 strengthens operational analyses, coordination, and expertise. Operating in this manner improves and strengthens law enforcement agencies capabilities in combatting online CSA (European Parliament of Justice, 2015). In 2015 an expert Academic Advisory Board was set up to advice the EC3 on research in the cybercrime area including online CSA.

A global alliance was launched in 2012 in which 54 European and other countries such as the US made commitments on concrete actions against combating online CSA. This alliance aims to: 1) Enhance efforts to identify victims and ensure they receive the necessary assistance, support, and protection; 2) Enhance efforts to investigate cases of child sexual abuse online and to identify and prosecute offenders; 3) Increase awareness among children, parents, educators and the community at large about the risks; 4) Reduce the availability of child pornography online and the re-victimization of children. Evident throughout these aims and objectives is Europe's prioritization in raising awareness concerning online CSA in

various communities. As a consequence of this joint vision, Insafe was founded; an international network including safer internet centres in European countries. These centres work together with industry, companies, and NGOs to increase awareness and prevent online CSA. Insafe intensively collaborates with INHOPE, an international network of helplines to report online CSA.

European networks and regulations set boundaries and provide assistance in fighting online CSA at by country level. They face the same difficulties in policing online CSA in contrast with offline CSA cases. Combatting online crimes has certain advantages compared to offline crimes, such as being able to identify an offender in another country which is not physically close, but it certainly also has its downside. Difficulties entail technological challenges faced during policing online CSA, such as encryption, but also as discussed before differences in legislation across countries with regard to online CSA (Davidson & Gottschalk, 2010). Collaboration between countries can be a serious challenge in policing these kinds of cases but is also essential in combatting online CSA. On a national level, police investigators have to handle reports and criminal events of online CSA filtered down from Europe and from the National Centre for Missing and Exploited Children (NCMEC) in the US. There are vast differences in how the police organize this process. The following section will outline the way in which police forces are organized in the United Kingdom, the Netherlands, Ireland and Italy to combat online CSA.

With regard to the United Kingdom, online CSA is largely investigated by specialized units. Most police forces in the UK have specialized teams that deal with the detection of online CSA. This allows the police to gather expertise but this also prevents the rank and files police officers experiencing an overload of CSA case in the regular operations unit (DeMarco & Davidson, 2015). In the UK, this is mostly led by the Child Exploitation and Online Protection Centre (CEOP), formerly the Child Exploitation and Online Protection Centre. The CEOP consists of three core modules; intelligence, operations, and harm reduction (DeMarco & Davidson, 2015; https://ceop.police.uk/About-Us/). Victims can directly contact CEOP when there is an issue with regard to the safety of young people online. The aim is to minimise bureaucracy and simplifies the way in which victims can seek support and assistance (DeMarco & Davidson, 2015). Police in the UK also aim to prevent online CSA by raising awareness among parents and children mostly by collaborating with educational institutes and providing awareness material on the CEOP website (https://ceop.police.uk/Knowledge-Sharing/). As a main focus, CEOP prioritizes concerns about technological and safety education on the internet for young people. CEOP also educates young people via their website providing safety information for a broader public than young people only. Specifically, teachers, law enforcement, and others who are interested can find information concerning online CSA on the CEOP ThinkUKnow website.

In the Netherlands, policing online CSA is also mostly handled by specialized teams that were created to combat both on- and offline CSA. There are two specialist teams that collaborate closely: The team focusing on sexual offences (team zedenzaken) and the team focusing on child pornography and child sex tourism (TBKK). These teams consist mostly of experienced police officers who received additional training for CSA cases and receive the necessary means and help to deal with these complex cases of (online) CSA. These teams are organized both regionally and nationally. The national TBKK is involved in more complex cases and digital investigations. All cases concerning sex offences against minors, either online or offline, are supposed to be redirected towards the specialized teams. This should ensure that officers who handle these delicate cases are specialized in the field of online CSA. Local police officers in the Netherlands are also involved in education programs in which they educate young people about online dangers with the goal of prevention. The police in the Netherlands collaborate closely with NGO's Helpwanted (a helpline) and Meldknop.nl (a hotline), which are both part of the European network of Safer Internet Centres. This allows young people to receive advice and help when there is a threat of becoming a victim or when they have been victimized from online CSA. In general, these organizations are easier and accessible to approach for youngsters in contrast to directly reporting a case with the police.

In Italy, Postal and Communication Police Service, a special branch of Italian National Police, which is based in the Department of Public Safety, has a specialized team with concern to online CSA. It is called the National Centre for Combating Online Child Pornography (CNCPO). Among other things, CNCPO manages a black list in order to block dangerous sites. The Centre collaborates with other Italian Police forces (such as Carabinieri) and with several NGOs, including two Italian NGOs within the Safer Internet Centre that are an initiative of the European Commission: SOS Il Telefono Azzurro Onlus and Save the Children-Italy. Both Il Telefono Azzurro and Save The Children-Italy manage hotlines (Clicca e segnala and Stop-It). Episodes of online CSA, dangerous and potentially risky materials, and child pornography materials can be reported to the CNCPO through these hotlines. There is an increasing collaboration with INHOPE, an organization fighting against online pornography by tracing the websites and their respective hosting countries that are reported as dangerous due to their contents. The Italian legislation in this field now recognizes the crime of online grooming (Italian law 172/2012). Postal and Communication Police recently received the possibility to investigate grooming cases undercover. Specialists in combating online CSA within the Postal and Communication Police force are trained in the use of advanced technologies, and receive support from CNCPO psychologists to deal with the potential difficulties.

Traditionally in Ireland, online child sexual abuse would mainly have been investigated by two specialist units, the Paedophile Investigation Unit (PIU) and the

Computer Crimes Investigation Unit (CCIU). Staff in these units will have been trained to at least detective level. The PIU also deals with offline forms of child exploitation, and the CCIU deals with any form of online crime. However, in more recent times, officers based in stations around the country are beginning to take a more active role in these investigations as they have been trained to forensically analyze mobile phone data. The PIU still has a level of involvement in such investigations, particularly by keeping a watching brief on all cases involving child abuse imagery- they receive reports from stations around the country and they upload any imagery to the ICSE DB. The PIU now take on the most complex or immediate threats, and large and/or sensitive investigations. An Garda Síochána work with the Office for Internet Safety, schools, charities, and children's services to deal with the issue of keeping children safe from abuse.

Although global alliances between countries are inevitable, collaboration between law enforcement and NGO's is not enough in combatting online CSA. Another important agent are industry organizations themselves; such as Social network sites and internet providers. As seen in the previous section from the stakeholder interviews, collaborations between law enforcement and industry seems difficult. However, collaboration is inevitable in the fight against online CSA. An example of such a collaboration between law enforcement, industries, and NGO's is the Advisory board of INHOPE in which all of these are represented and united against online CSA (e.g. EC3, Interpol, Microsoft, ECPAT). Altogether, European networks and regulations guide the way in which member countries police online CSA in collaboration with involved stakeholders such as industries and NGOs.

4.2 Policing Online CSA: Descriptive findings from surveys

The following section will provide an overview of descriptive findings from our police survey focusing on to 1) Experience with online CSA; 2) Specialism, training, and preparedness; and 3) Collaboration. For a more thorough description of the methodology applied in developing and analyzing the questionnaire, see earlier sections of this report. The questionnaire itself may be found in Appendix III.

Please note that because of differences in sample selection across countries (i.e., specialists/non-specialists, rank, gender), comparisons between countries should be interpreted with care, taking sample differences into account. Selection of the respondents did not take place randomly because of constraints set by the police organization in each country. In the UK, sampling was pushed widely across police forces and ranks, while in the Netherlands access was only gained to specialists. In Italy mostly general police officers were approached. Descriptive statistics by country are given but should not be used to compare countries in general, but can

be interpreted with the above mentioned considerations of sample differences taken into account.

Table A: Descriptive demographics of sample by country

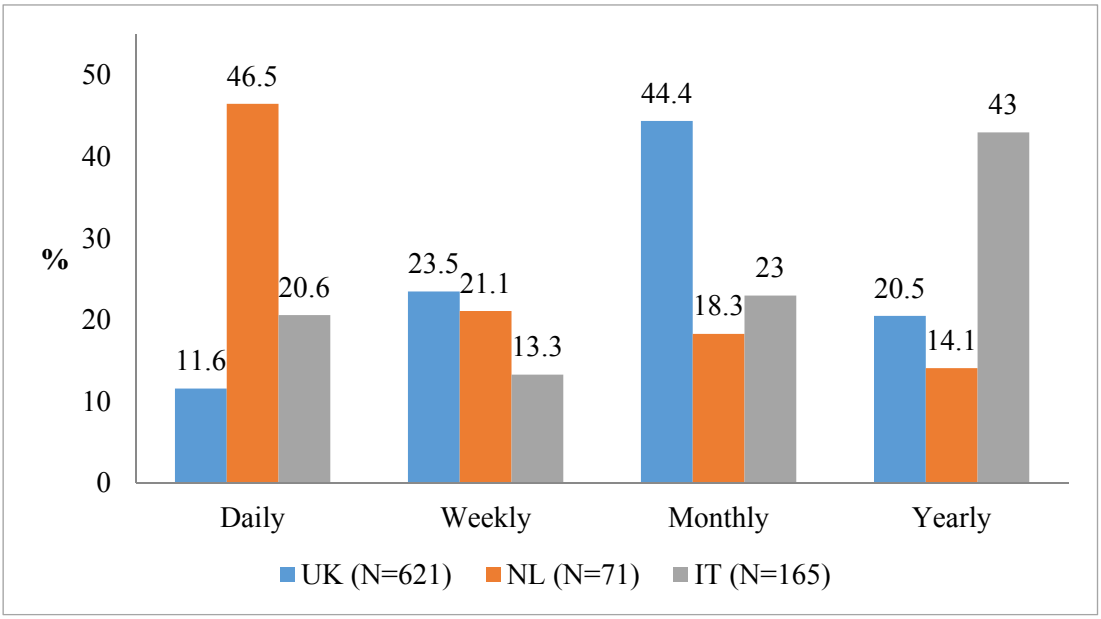
		Country		
	All	**United Kingdom**	**The Netherlands**	**Italy**
Male	70.6% (N= 888)	59.4% (N= 399)	58.8% (N= 57)	88.3% (N= 431)
Female	29.4% (N= 370)	40.6% (N= 273)	41.2% (N= 40)	11.7% (N= 57)
Mean age (years)	43.22 (SD= 8.06)	41.24 (SD= 7.86)	46.18 (SD= 9.55)	45.43 (SD= 7.24)
Length service (years)	18.98 (SD= 9.36)	15.86 (SD= 8.31)	22.50 (SD= 11.57)	22.83 (SD= 8.57)
Current role (months)	45.28 (SD= 56.33)	37.45 (SD= 44.21)	65.11 (SD= 57.47)	52.63 (SD= 68.64)
Note. N = number of participants, SD = standard deviation of the mean				

Experience with online CSA

The following section will outline the amount of experience police officers in the sample had with regard to cybercrime. The majority of the police officers (68.9%, N= 861) answered that they have encountered a form of cybercrime during their service. In response to the frequency of encountering cybercrime during their work, it seems that 16.2% (N= 139) are engaged with cybercrime on a daily basis. Others encounter cybercrime weekly (21.4%, N= 184), monthly (38.1%, N= 327), or yearly (24.3%, N= 209). See Figure 4.1 for descriptive statistics regarding encountering cybercrime by country. It becomes clear that the Dutch sample more frequently encountered cybercrime on a daily basis, whereas police officers in the UK and Italy experience this respectively more on a monthly and yearly basis. This makes sense considering that the Dutch sample is a specialist team in online CSA.

According to one of the interviewed Irish Detective sergeants, front officers in Ireland are not regularly exposed to cybercrime. However, they are increasingly coming into contact with such crimes. No specific statistics are available from the Irish police at the time of the current research as to the incidence of crimes with a significant cyber element due to the current system of reporting and recording crimes within traditional classifications.

Figure 1. *Police officer encounters with cybercrime by country*



When asked about dealing with multiple forms of cybercrime over the last ten years, the most encountered cybercrimes were the collection and distribution of online CSA material and grooming cases. Among the least common online CSA cases that police officers encountered were trolling (verbally upsetting others online) and flaming (posting online messages which are insulting), less than one out of five officers experienced these kind of cases. For results see Table B.

Both Detective Sergeants included in the Irish sample had personally been involved in online child sexual abuse investigations involving: image collection, production and distribution, online grooming, arranging/facilitating commission of a child sexual offence, voyeurism and sexting. They have both had cases involving online harassment, cyber-bullying, impersonation/identity theft and masturbation/ exposure to minors via webcams and one has been involved in cases of minors being exposed to indecent images of children. Incidences of trolling or flaming were unknown. Traditionally, front-line officers would have had limited involvement with such investigations due to the policy of referring these cases to senior staff and due to the pivotal the role of the specialist units. However, in more recent times, they are becoming more involved in investigations. According to the Detective Sergeants interviewed, front-line officers in local stations would mostly be exposed to cases involving sexting – underage self-generated sexual images or videos.

Table B. *Investigations of online offenses encountered in last ten years*

	Country			
	All	**United Kingdom**	**The Netherlands**	**Italy**
Collection material	44.7% (N= 527)	61.6% (N= 386)	77.7% (N= 73)	14.5% (N= 66)
Distribution material	43.0% (N= 506)	60.1% (N= 377)	79.8% (N= 75)	11.4% (N= 52)
Grooming	42.5% (N= 501)	61.6% (N= 386)	68.1% (N=64)	11.0% (N= 50)
Sexting	40.5% (N= 478)	60.0% (N= 376)	61.7% (N= 58)	9.2% (N= 42)
Production material	36.8% (N= 434)	50.7% (N=318)	72.3% (N= 68)	10.3% (N= 47)
Cyberbullying	32.7% (N=389)	46.3% (N= 290)	42.6% (N= 40)	12.2% (N=57)
Harassment	31.5% (N= 375)	42.6% (N= 267)	37.2% (N= 35)	15.4% (N= 72)
Online impersonation and Identity theft	21.3% (N= 254)	23.9% (N= 150)	24.5% (N= 23)	17.3% (N= 81)
Trolling	19.9% (N= 237)	24.9% (N= 156)	29.8% (N= 28)	11.4% (N= 53)
Flaming	12.9% (N= 153)	10.2% (N= 64)	23.4% (N= 22)	14.3% (N= 67)
Note. N = number of participants				

Furthermore, the type of evidence collected when police officers encounter a case of online CSA was explored. Information and Communication Technology (ICT) devices such as mobile phones, laptops, tablets, and hard drives take the lead in evidence that is collected, while less than one third of the police officers claim that character statements are collected in investigations concerning online CSA. One country difference in evidence collected seems noticeable. Gaming consoles in the UK seem to be regularly collected as evidence in online CSA cases (70% of police revealed), while this is the case in only one third of the cases in the Netherlands and one fifth of the cases in Italy. For all results see Table C.

With regard to evidence collected in online CSA cases in Ireland, mobile phones, tablets, gaming consoles, laptops, hard-drives, DNA evidence, finger prints, witness, and character statements are all collected.

Table C. *Evidence collected when encountering online CSA*

	Country			
	All	**United Kingdom**	**Netherlands**	**Italy**
Mobile phones	95.5% (N= 750)	98.0% (N= 580)	77.0% (N= 67)	97.2 (N= 103)
Laptops	93.2% (N= 732)	95.8% (N= 567)	77.0% (N= 67)	92.5% (N= 98)
Tablets	91.6% (N= 719)	94.3% (N= 558)	77.0% (N= 67)	88.7% (N= 94)
Hard drives	89.8% (N= 705)	92.7% (N=549)	75.9% (N= 66)	84.9% (N= 90)
Witness statements	88.3% (N= 693)	93.4% (N= 553)	70.1% (N= 61)	74.5% (N= 79)
DNA (blood/semen)	69.4% (N=545)	78.4 % (N= 464)	50.6% (N= 44)	34.9% (N= 37)
Gaming consoles	60.2% (N= 472)	70.9% (N= 420)	34.5% (N= 30)	21.0% (N= 22)
Fingerprints	60.0% (N= 471)	69.4% (N= 411)	26.4% (N= 23)	34.9% (N= 37)
Character statements	40.1% (N= 315)	32.9% (N= 195)	32.2% (N= 28)	86.8% (N= 92)
Note. N = number of participants				

Specialism, training, and preparedness

The degree of specialty and police officers role description was explored via several items, including: *'Are you a specialist in the field of online CSA'*, *'Are online CSA cases always referred to specialized teams'*, and whether or not they were familiar with national and international guidelines with concern to online CSA. Sample differences are evident, with specialists highest in the Dutch sample as already discussed. One-third of the Italian police officers, which mostly composed of general police officers, indicated that they are a specialist in online CSA. Another noticeable difference is the way that police organizations seem to process online CSA cases. In the Netherlands these cases are mostly referred to specialist teams while this is less the case in the other countries. For results see Table D.

Table D. *Specialism and familiarity with legislation*

	Country			
	All	**United Kingdom**	**The Netherlands**	**Italy**
Self-indicated specialist	26.9% (N= 334)	12.1% (N= 82)	88.7% (N= 86)	35.5% (N= 166)
Cases are always referred to specialists	88.7% (N= 86)	59.1% (N= 387)	98.6% (N= 63)	13.4% (N= 63)
Familiar with national legislation [a]	62.9% (N= 680)	99.6% (N= 498)	88.4% (N= 84)	20.0% (N= 97)
Familiar International legislation [b]	7.1% (N= 77)	4.2% (N= 21)	33.0% (N= 32)	4.9% (N= 24)

Note. n = number of participants

[a] In Italy, a law concerning online grooming (Law C.P. 172/2012) was approved on October 2012, this can explain why less police officers in the Italian sample (mostly composed of general police officers) were familiar with national legislation.

[b] Knowledge about international legislations included the international guidelines child abuse 2013, this can explain why less police officers indicated that they were familiar with the international guideline.

A question on whether or not police officers received any training on online CSA was also included. Results are shown in Figure 2 of the total sample, and in Figure 3 by country. It is noticeable that the majority of the police officers (61.0%, N=776) indicated that they did not receive any training concerning online CSA. The percentage of untrained police officers in online CSA is the highest in Italy (86.5 %). However, it is also noticeable that in the Dutch sample, that consists of specialists, more than one third indicated that they did not receive any training on online CSA.

Figure 2. *Police training on online CSA*

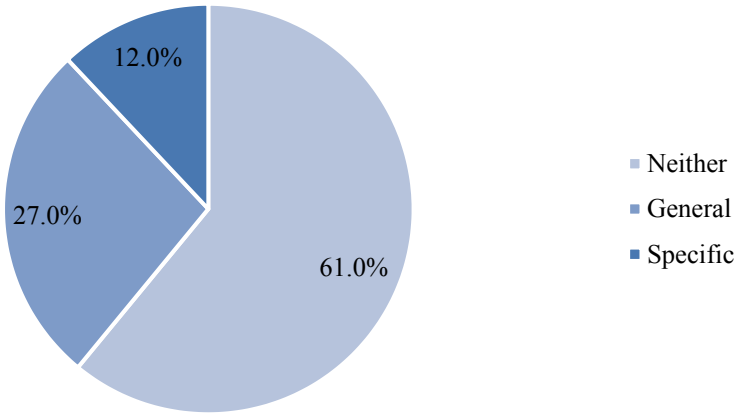
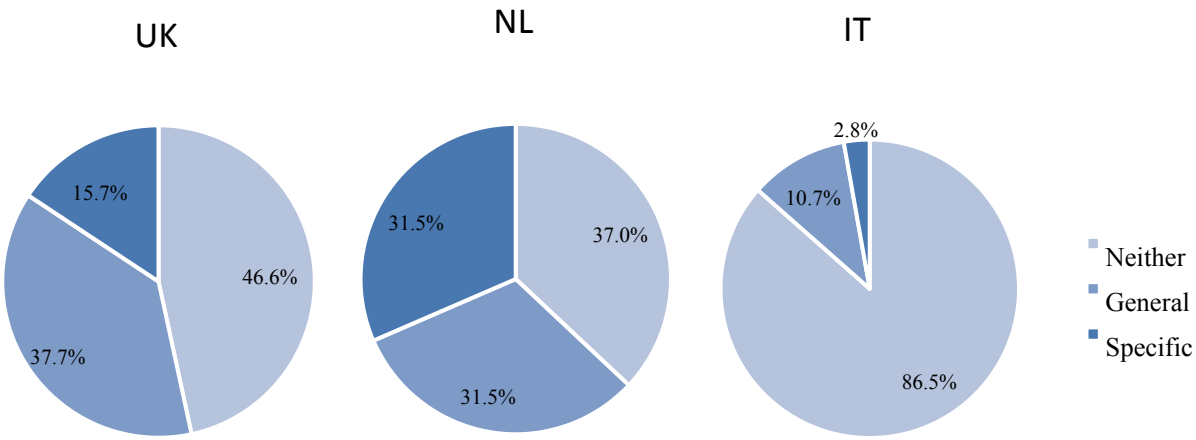


Figure 3. Police training on online CSA by country



Questions regarding the quality of the training were asked, including: *'How would you describe the quality of the training?'* and *'How prepared do you feel as a consequence of the training'*. Results are shown in Figure 4 and 5 respectively. More than half of the participants who did receive training indicated that the training was adequate. However, there is also a large number of police officers (approximately 40%) who claimed that their training was poor. When asked how prepared officers felt as a consequence of their training, *'extremely prepared'* is the answer that is most often provided (four out of ten).

Figure 4. *Description of police training on online CS, role specific*

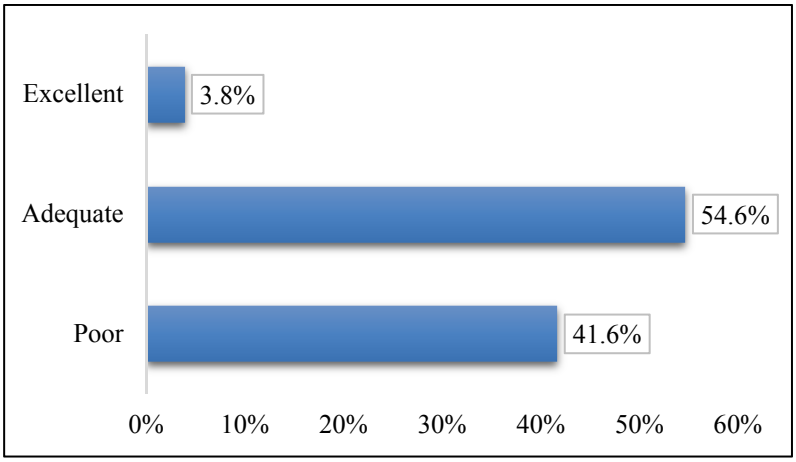
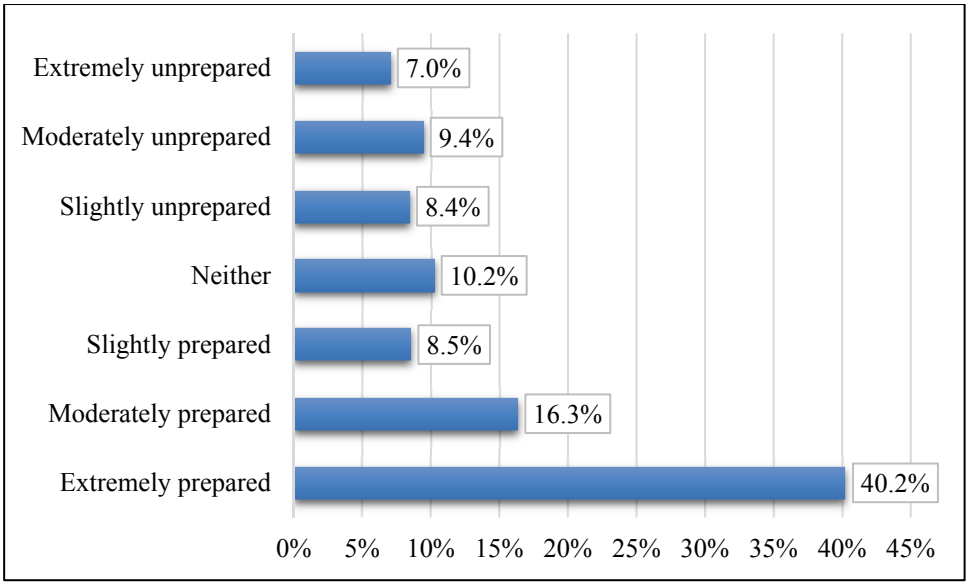


Figure 5. *Training preparedness by police officers*



An Irish perspective on training and specialism in online CSA cases was also included in the mixed method approach. Over the past 10 years, investigations into online child sexual abuse would for the most part have been dealt with by the Paedophile Investigation Unit and the Computer Crimes Investigation Unit. Staff in these receive specialist training in online investigations into childhood sexual abuse. This training includes Europol's annual training course on Combatting Sexual Exploitation of Children on the Internet (COSEC). Europol's COSEC ten day training consists of lectures and practical exercises delivered by international expert trainers and guest lecturers. The Detective Sergeants interviewed referred to the intensity of this course, and with that, the benefit to learning that comes with such an intensive course. One particular positive that was highlighted about the COSEC course, was that it is well-tailored. Even though people may come to the training at different levels of knowledge, everyone reaches the same goal by the end of the training. Other training is funding-dependent, and includes the European Police College's

(CEPOL) online sexual abuse courses and national training on specific topics, e.g. Mentor Forensics' training on understanding sex offenders. Additionally, a number of staff in the units have been trained on victim identification and the International Child Sexual Exploitation image database (ICSE DB), expertise which they can share with other staff. In general, the Detective Sergeants were extremely positive about the courses they attended – "Brilliant, brilliant, brilliant" and "We're very happy with the training" specifically mentioning the benefits of the courses being dynamic and changing according to new trends in techniques or evidence. Similarly, the utility of these training courses in terms of networking and building relationships with law enforcement worldwide was mentioned, particularly beneficial given the cross-jurisdictional nature of online child sexual exploitation. One recommendation put forth regarding training for staff was to be given the opportunity to attend more training courses.

Partnership and collaboration

As outlined earlier in this chapter, collaboration between the police and other professionals are critical in the fight against online CSA. Therefore, questions were administered concerning the amount and the type of collaboration that police forces had with others such as social workers, industries, and other organizations throughout investigations (see Table E) and during the general prevention and intervention of online CSA (see Table F). It is noticeable that ***Education*** is most often named as a partner in investigations and collaborating. According to the participating police across the nations, industries are often not stated to be a collaborating partner (20%).

With regard to collaboration in online CSA cases in Ireland, child protection teams are always involved in online CSA investigations. This is mandatory according to Ireland's Children First National Guidance for the Protection and Welfare of Children. The Irish police and Tusla, Ireland's Child and Family Agency are the two agencies with statutory responsibility for child protection (An Garda Síochana, 2013). Generally, the two main professions involved with the investigation outside the police are the social workers and psychologists employed by Tusla. Other professionals would only be involved if they were directly relevant to an investigation. One recommendation put forth by a Detective Sergeant to improve this partnership was to have specialist staff in Tusla dedicated solely to child sexual abuse.

An Garda Síochána also run a program whereby trained members visit schools to address the topic of internet safety. Relationships with victim support groups and other charities such as Barnardos, the Rape Crisis Network and One in Four are largely in relation to contact child sexual abuse. Collaborations also include national

law enforcement and international law enforcement agencies to assist in investigations through information sharing, as well as NCMEC. Collaborations also exist with technology companies in Ireland. This relationship is based on information transfers – technology companies may report illegal content to The Irish police, or the police may request information from a company about a user's activity where relevant to an investigation. Also meetings with representatives from a number of large technology companies who have formed a User Protection Forum are organized, in order to inform companies about the points of contact within the Irish police.

Table E. *External police partnership involved in investigations*

	Country			
	All	**United Kingdom**	**Netherlands**	**Italy**
Education	51.0% (N= 417)	54.6% (N= 337)	43.2% (N= 38)	36.4% (N= 40)
Victim support	48.5% (N= 396)	54.5 % (N= 336)	46.6% (N= 41)	16.5% (N= 18)
Medical professionals	42.6% (N= 348)	51.1% (N= 315)	36.4% (N= 32)	0.9% (N= 1)
Child protection teams	35.0% (N= 299)	31.1% (N= 209)	15.5% (N= 15)	68.2% (N= 75)
Psychologists	27.1% (N= 221)	19.6% (N= 121)	27.3% (N= 24)	68.2% (N= 75)
Note. N = number of participants				

Table F. *Collaborations with non-police in dealing with online CSA*

	Country			
	All	**The United Kingdom**	**The Netherlands**	**Italy**
Education	62.0% (N= 431)	70.7% (N= 352)	41.4% (N= 36)	39.1% (N= 43)
Charities / NGO's	35.8% (N= 249)	40.0% (N= 199)	29.9% (N= 26)	21.8% (N= 24)
Victim support	32.4% (N= 225)	35.9% (N= 179)	36.8%(N= 32)	12.7% (N= 14)
ICT/Industry	22.0% (N= 153)	17.3% (N= 86)	47.1% (N= 41)	23.6% (N= 26)
Probation	19.0% (N= 132)	20.5% (N= 102)	31.0% (N= 27)	2.7% (N= 3)
Note. N = number of participants				

4.3 Inferential Analyses

Examining police abilities

Stratified random sampling was not possible for the surveys, thus the results with respect to countries are not directly comparable. On one side, participants' responses were likely to be influenced by relevant clustering effects (e.g. almost only specialists in online CSA participated in the study in the Netherlands), which limited the possibility to compare police practices across countries. However, the high variability in responses and respondents across countries allowed us to treat sample

data as a whole, and thus to examine some relationships and associations between variables, considering the differences in sample selection.

In order to achieve a better understanding of the relationships between the investigated variables both univariate and multivariate techniques were used, for example to test whether having received a specific training for the investigation of online CSA was related with questioning child victims about their online behaviours. Univariate statistics involved tests such as Pearson's chi-square to examine the association between variables, and t-tests for independent samples or analysis of variance (ANOVA) to examine differences between groups. We relied on multiple correspondence analysis (MCA) for multivariate analysis. MCA is a special technique of data analysis for multivariate categorical data, and it is used to detect and represent underlying structures in a data set.[1] This method was particularly appropriate for investigating our sample data, because many of the variable responses in the study were categorical (e.g. yes or no), and because this specific analytic technique allows researchers to check for potential clustering effects without necessarily including these effects in the statistical models.

Testing for sample selection differences

It was already clear that participants were selected according to different criteria across countries, but examining how these differences in sampling selection related with reported experiences on policing online CSA was critical for further analysis. For example, we observed that there were significant differences with respect to gender and age of participants across countries: female police officers were 41.2% (40/97) and 40.6% (273/672) in the Netherlands and in the UK, respectively, while they were

1 In summary, the MCA technique preserves the categorical nature of the variables, since the analysis is conducted at the level of the response categories rather than at the variable level. Associations between variables are examined by calculating the chi-square distance between different categories of the variables and between the individuals. Inertia, a measure of deviation from independence which is directly related to Pearson's chi-square statistic, is in fact used as a measure of dispersion of the individual profiles around the average profile. The larger the differences are, the larger the inertia will be. Dimensions are formed by identifying those axes for which the distance between the profiles and axes is minimized, while the amount of explained inertia is simultaneously maximized. So, if two categories have similar count patterns, their profiles will be close together in the joint plot that is used to visualize the results of this analysis. Therefore, MCA was used in this context because: (1) this data analytic procedure allows researchers to simultaneously manage multiple categorical variables; (2) it generates data-driven quantifications and representations of the similarities and differences across participants according to their responses; (3) has the advantage of plotting together these similarities and differences on a graph, which facilitates a comprehensive understanding and interpretation of data. Classical rules, such as retaining a dimension only if its eigenvalue was above 1, and retaining a number of dimensions which represent more than 70% of the inertia, were applied for the report. We attributed a tentative name to the first two dimensions (displayed through x and y axis in the joint category plot) of the MCA performed, as the first two dimensions of MCA always have the highest eigenvalues and explain the largest amount of inertia.

only 11.7% (57/488) in Italy. Moreover, UK police officers were younger than Dutch and Italian police officers ($F(2, 1251)=48.45$, $p<.001$), and their length of service in the police force was shorter than Dutch and Italian participants ($F(2,1232)=96.82$, $p<.001$). These different sample characteristics may of course reflect differences in police recruitment policy across countries, but it is also likely that they actually reflect the differential responses to our survey by police forces across countries. An example is that because of the inclusion of almost only specialists in the Dutch sample, they also have a longer period of service on average.

In fact, it was verified that country differences in sample selection were evident in terms of experience , competence and training for investigating and policing online CSA: 88.7% (86/97) in the Netherlands, 35.5% in Italy (166/468), and 12.1% (82/678) in the UK defined themselves as specialists in online CSA. This difference was highly significant: $\chi^2=281.40$, $df=2$, $p<.001$. However, general or specific training for investigating online CSA was quite poor in the Italian sample (13.5%, 63/469), with respect to the UK (53.4%, 361/676) and Dutch samples (63%, 58/92): chi-square(2)=210.23, $p<.001$. Moreover, almost all of the UK police officers who participated in the study had to deal with any form of cybercrime before (91.2%, 619/679), more than Dutch participants (74.2%, 72/97), while only a third of the Italian respondents reported any investigation on cybercrime (35.7%, 168/471): $\chi^2=400.98$, $df=2$, $p<.001$.

These differences demonstrate the diverse characteristics of the country samples, but at the same time they confirm that a wide range of experiences concerning training and investigation of online CSA were reported in the entire sample. This rendered the analysis on these experiences as a whole particularly relevant for the development of best-practice models and effective policies to improve the fight against online CSA.

Dealing with cybercrime across police ranks

Together with those who specifically operate in specialized structures for undercover work and detecting online child sexual abuse (80%, 4/5), chief constables (72.2%, 13/18) and detective chief inspectors (63.6%, 7/11) were those who more frequently reported to deal with cybercrime on a weekly or daily basis ($\chi^2=42.23$, $df=16$, $p<.001$). This suggests that high levels of experience in the police are needed to effectively deal with cybercrime. However, it should be highlighted that the prevalence of dealing frequently with cybercrime (i.e. at a daily or weekly basis) was reported across all ranks, with the lowest prevalence being 15.4% across chief superintendents. This could suggest that cybercrimes are so widespread in modern policing that almost all police offers have to deal with them. In this context, it is noteworthy that 90.8% (556/612) of the respondents who reported dealing with

cybercrime at least on a yearly basis considered it as very important that their police forces management had an understanding of online CSA in order to facilitate investigations. Only 1.4% (9/612) of those who dealt with cybercrime at least on a yearly basis considered understanding of online CSA as unimportant or neither important nor unimportant. This difference was highly significant (χ^2=983.45, df=1, p<.001).

Training, preparedness, and quality of investigations in online CSA

An ANOVA with Scheffé's post-hoc test for comparisons between groups showed that those who received specific training on investigating online CSA described their role-specific current training surrounding the policing and investigation of online CSA as more adequate than those who received general training. In turn, the ones who received general training perceived themselves to be better trained than those who did not receive any training ($F(2, 1095)=291.04$, p<.001).

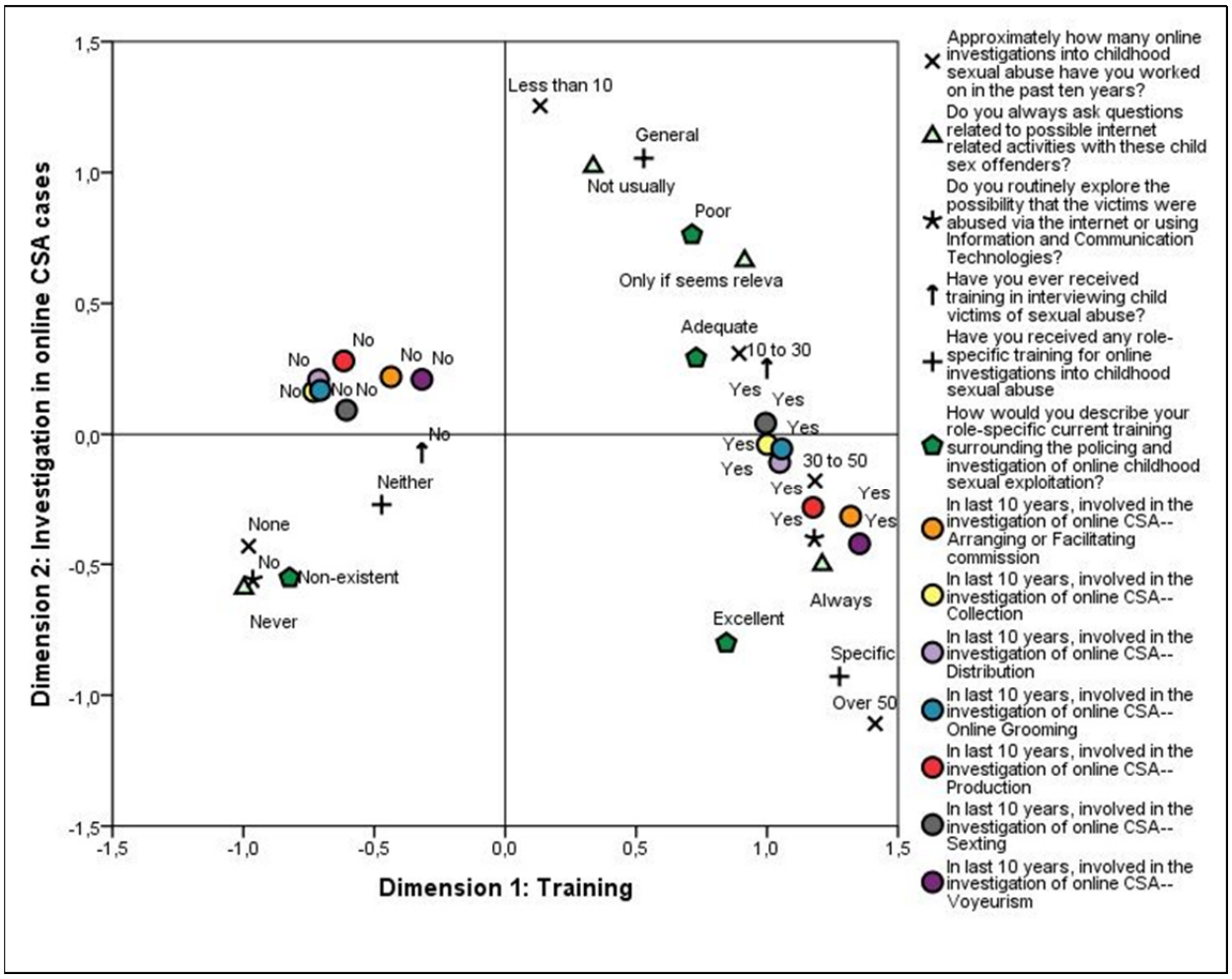
This dose-response effect concerning training was expected, but surprisingly it was not reflected in the groups' perception of their preparedness. Another ANOVA with Scheffé's post-hoc test showed that those who received specific training and those who did not receive any training perceived themselves to be more prepared on the topic of online CSA than those who received a general training ($F(2, 1091)=32.28$, p<.001).

This surprising result led to an exploration of whether the perception of preparedness among police officers who were not trained might be biased, for example by a shortage of knowledge concerning online CSA. Therefore, the extent to which there were group differences in participants' knowledge of national and international laws on online CSA was explored, about half of those who did not receive any training on policing and investigation of online CSA were familiar with national legislation in this area (43.2%, 281/651), while those who received general or specific training had in almost all cases sufficient knowledge about national laws on online CSA (97.1% and 96.3%, respectively). This difference was significant (χ^2=314.79, df=2, p<.001), and found replication for what concerns international laws. Only 4.2% (32/651) of those who did not receive any training were familiar with international laws, compared to 8.7% (24/276) of those who received general training and 15.6% (21/135) of those who received specific training (χ^2=19.98, df=2, p<.001).

Therefore, this difference suggests that the perception of preparedness among those who were not trained in dealing with online CSA could be biased. This finding may have relevant implications, as those who were not trained, if they perceived themselves as sufficiently prepared, could be less likely to detect potential cases of

online CSA. Further analysis was conducted to explore the relationship between training in dealing with online CSA, actual investigation on online CSA, and actual behaviours during the investigation. A MCA was performed in order to examine this relationship. The result of this analysis is presented in Figure 4.6 (inertia explained=73.7%).

Figure 6. *Cybercrime, training experience, and investigations*



As Figure 6 suggests, those who were often involved with online child sexual abuse received a specific training, perceived themselves as excellently or at least adequately trained, and in most cases explored the online risks in child victims and investigated the online behaviours of offenders (see the lower right side of the graph). Those who were not trained and had not been involved in investigations on this type of crime actually do not usually explore the online behaviours of victims and offenders (left side of the graph). This might strongly limit their ability to detect and deal with online CSA. Moreover, there is a group (represented in the upper right corner of the graph) who did deal with online CSA, though less frequently than the first group, but received only generic training and had the perception of having been poorly prepared to work on online CSA cases. This important finding suggests that it is important to improve the skills of these officers in order to better equip them for dealing with online CSA.

Sensitive approaches to victims and offenders

It was observed that while there were no significant differences between male and female police officers with respect to their specialization in online investigation of CSA (26.5% among females and 27.1% across males (χ^2=0.42, df=1, p=.84, n.s.). Females reported being involved in more investigations of online CSA cases during the last ten years (a mean of 19 cases) than did respect to males (a mean of 13 cases). This difference was statistically significant (t(1196)=4.68, p<.001). This finding was explored further and it was discovered that more females than males were trained in interviewing victims of child sexual abuse (40.4% against 16.3%, χ^2=78.29, df=1, p<.001). Often this training among females also involved interviewing and dealing with victims of online CSA (15.6% against 6.6% among males, χ^2=14.78, df=1, p<.001). However, the findings also indicate that female participants were more likely than males to explore whether child victims were abused via Internet or using ICT (46.7% against 14.9%, χ^2=53.16, df=1, p<.001). Also, females more often (40% against 18.1% among males) responded that they always ask questions of child sex offenders concerning possible Internet related activities (χ^2=103.46, df=1, p<.001). There were no significant differences between males and females on the importance attributed to the understanding of the manager of online CSA in facilitating investigations in this area (t(654)=.21, p=.83, n.s.).

Practices and collaboration

It is noteworthy that only 1 out of 4 of those who said that they conduct specialized interviews with victims of CSA reported having been trained to deal with victims of online CSA (23.7%, 42/177). Moreover, the results suggest that the group conducting specialized interviews with victims of CSA were also more likely than other participants to interview child sex offenders (89.3%, 184/206): χ^2=462.54, df=1,

p<.001. The analysis of this subgroup was therefore particularly important in order to understand how the officers who are most involved in CSA investigations, are also involved through interviews with the psychological health of the child, usually deal with online CSA. The findings also shed light upon the way in which they perceive the current situation involving training and collaboration. Chi-square analyses showed that this subgroup reported higher levels of collaboration with child protection teams (χ^2=22.51, p<.001), social workers (χ^2=98.70, df=1, p<.001), psychologists (χ^2=23.73, df=1, p<.001), victim support services (χ^2=49.34, df=1, p<.001), representatives from education (χ^2=51.14, df=1, p<.001), and medical professionals (χ^2=33.89, df=1, p<.001), for example. This suggests that the vast majority of the respondents in this subgroup are aware of the social resources that can help in improving investigations and at the same time supporting child recovery. However, while social workers are almost always involved (88.7%, 181/204), other potentially relevant figures are much less likely to be involved, such as psychologists (31.4%; χ^2=139.26, df=1, p<.001) and other victim support professionals (54.4%; χ^2=58.81, df=1, p<.001). Also, this subgroup more frequently reported the need for higher levels of collaboration with ICT and industry partners. In fact, in this subgroup the prevalence of positive responses on the questions concerning the usefulness of collaborative partnerships and the improvement of collaborative practices were often 2x the positive responses of those who did not directly interview child victims, with all chi-square differences significant (all p<.001). For example, 76.3% of this subgroup versus 41.3% of the other police officers believes that better data sharing among police and industries will improve effective partnerships between police and industries. Furthermore, 82.1% of this subgroup compared to 41.8% of the others believes that there is a need to improve communication between police and industries. Also, 72.3% of this subgroup against 32.3% of the others believes that seminars and lectures can improve collaborative practices, and this pattern of differences is observed also with respect to responses concerning the usefulness of developing joint task-force and secondments for policy and industry. Another MCA, presented in Figure 7, assists illustrating these findings more comprehensively (inertia explained in the model: 75.8%).

Figure 7. *Improving collaborative practices*

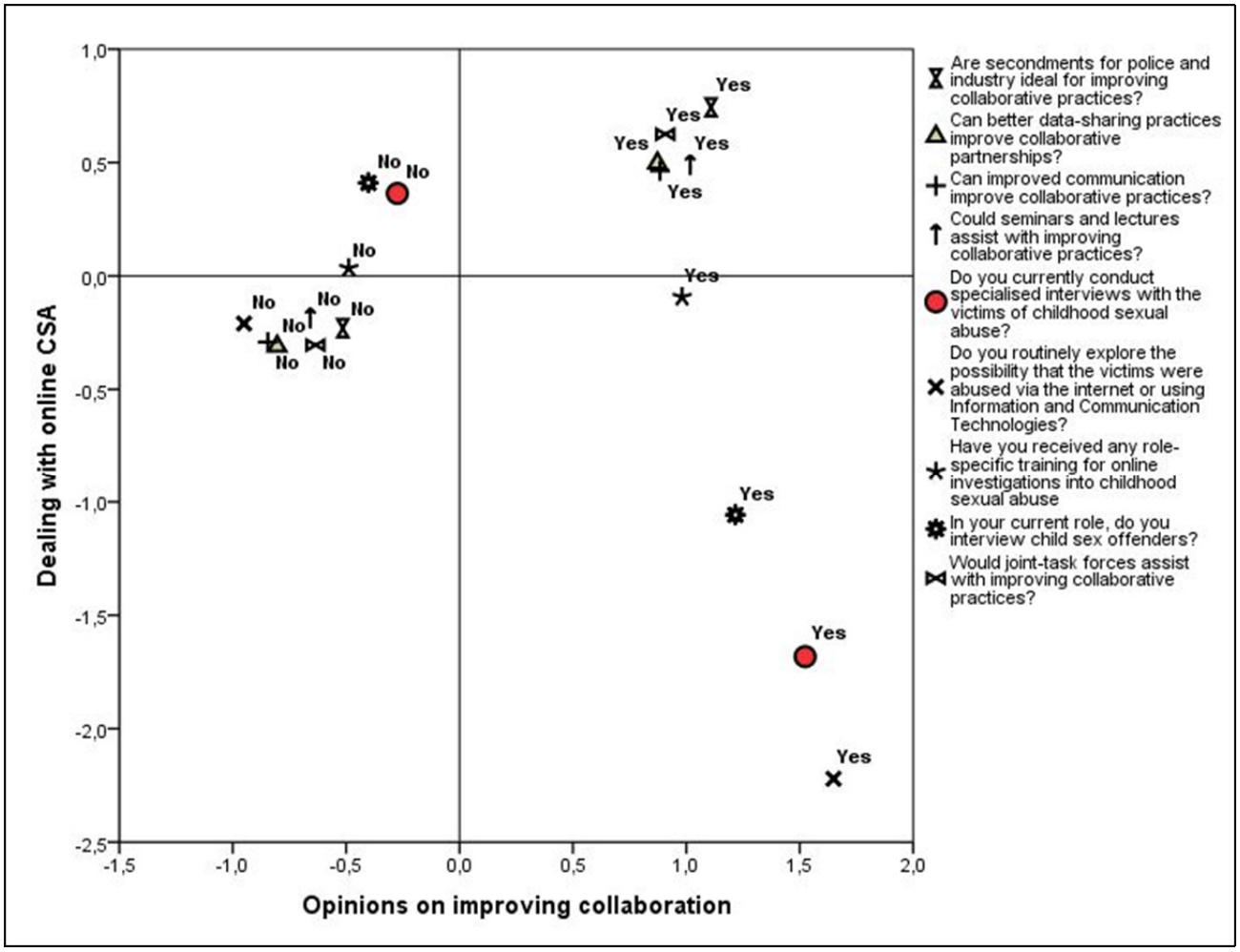


Figure 7 can be explained on the basis of the *x* axis, where there is a clear polarization of responses concerning the perceived usefulness of collaborations between police force and industries to increase knowledge and the quality of investigation in online CSA. In fact, while the *y* axis is mostly defined by categories concerning whether or not police officers usually performed specialized interviews with victims and offenders, the *x* axis describes police officers' opinions about the usefulness of further training (seminars and lectures) and collaboration with industries. Notably, all the positive responses about the usefulness of collaboration and training are plotted in the right side of the *x* axis, where also participants who reported to be specialists in online CSA and who interview child victims and offenders are plotted. This indicates that experts in online CSA consider improving collaboration and training as fundamental for combatting online CSA.

4.4 Summary

In this section, we have reported on policing practice on online child sexual abuse (CSA) across the UK, Italy, Ireland, and the Netherlands. We also described the results of a survey conducted in the UK, Italy, and the Netherlands, complementing quantitative findings from the survey with in-depth interviews with experts on policing online sexual offences from Ireland.

There are differences in policing cybercrime and online child sexual offenses across countries, which most likely reflects different traditions in legislation and police practice across the countries. However, some major points of convergence in fighting online CSA across the countries are observed. These concern: (a) a strict collaboration with overarching structures such as the EC3 Unit of Europol; (b) a collaboration with NGOs and industries, and the development of related national and international protocols that serve to combat online sexual offences in the country and across countries; (c) the increasing importance of specialized units within the police force that are able to effectively deal with, and fight against, cybercrime ;(e) a shared desire for specialist training and for effective collaborative partnerships , particularly with industry .

The results of the survey, despite the fact that they cannot be generalized to all the police forces in the partner countries because of the mixed-methodology and the different sample selection criteria, converge in illustrating that online child sexual offence is a widespread phenomenon. It is also illustrated that the fight against online CSA requires combined efforts by all partners involved (police, industries, NGOs, policy-makers, etc.) to be effectively contrasted. More in detail, it emerged from the survey that more than two thirds of the police officers in the entire sample had to deal with cybercrime at least once, and that approximately half of the respondents also had to deal with online child sexual offenses. This underlines the urgent need to address this type of crime effectively. Moreover, it emerged that role specialists and other police officers who frequently deal with online child sexual offenses suggest that training and collaboration with industries are fundamental in effectively investigating these cases. There was also evidence in the survey that effective training increases knowledge on these crimes (e.g., knowledge on specific country and international legislations), collaboration with services (e.g., with child protection teams, with social workers, etc.) and quality of approaches to victim and offenders (e.g., by asking child sexual abusers whether they also groomed a child online). The importance of training in this field is complemented by the importance of collaboration, as it emerged from the survey that about 3 out of 4 role specialists in dealing with online child sexual offenses believes that improved communication and collaboration with industries will help in combating online child sexual abuse.

Notably, such results are entirely consistent with the in-depth interviews conducted with role specialists in Ireland, and more generally with the stakeholders' perspective described in the previous section that improvements in training and collaboration between police and industries are needed to effectively prevent and combat online child sexual abuse. In summary, the results of the analysis on the policing practice across the partner countries confirm that a number of good practice examples have been developed to prevent and combat online child sexual abuse. Despite the amount of good practice there is still there a need to improve training and collaboration with other stakeholders. This could improve the identification of online child sexual offences and enhance the way in which such cases are dealt with to fight online child sexual abuse.

5.0 Youth online behaviour and risk

5.1 Theoretical context of online behaviours amongst digital natives

The availability and widespread use of digital technology has transformed the way in which we consider children and young people to be at risk of harm (Webster et al., 2012: Webster, Davidson & Bifulco, 2015). Internet usage is thoroughly embedded in the daily lives of children, with recent reports indicating that young people use the internet an average 17.2 hours per week (12-15 year olds) and that they are increasingly accessing the internet using smartphones (Ofcom, 2014). The rise of smartphones means young people can have immediate and unlimited access to the internet, making it increasingly difficult for their parents to monitor their online activities. Undoubtedly the online world poses risks for young people, such as cyberbullying, exposure to inappropriate material, and sexual exploitation. These are not entirely new risks faced by today's youth as, for example, bullying and sexual exploitation have long been societal problems. However, the issue is compounded by the fact that these risks now occur both offline and online, and that the anonymity of the internet can greatly facilitate deviant activities. In particular, the internet provides opportunities for sexual offenders to act in certain ways online, that they might be able to effectively suppress in the real world (Babchishin, Hanson & Hermann, 2011).

The aim of this element of the research was to identify factors associated with young people being at increased risk of online sexual exploitation, specifically, grooming. According to the European Online Grooming Project, online grooming is defined as the "process by which a person befriends a young person online to facilitate online sexual contact and/or a physical meeting with them, with the goal of committing sexual abuse" (Webster et al., 2012. p. 5). Due to a lack of representative studies, varying legislation worldwide, online anonymity and an estimated large amount of unrecorded cases, the exact prevalence of online grooming is unknown (Wolf, Wachs, & Pan, 2012). However, as grooming begins with an initial contact, studies on the receipt of online sexual solicitations by youth, including sexual messages and requests, can provide us with first indications of the issue.

Landmark research of 10 to 17 year olds in America found that between 13% and 19% of youth had received an unwanted online sexual solicitation in the year previous (Finkelhor, Mitchell, & Wolak, 2000; Wolak, Mitchell, & Finkelhor, 2008). Similarly, recent research using a European sample indicated that 15% of 11 to 16 year olds had previously received sexual messages, with 25% of this sample stating that they were upset by this (Livingstone, Haddon, Gorzig & Olafsson, 2011). However, the proportion of these messages sent by adults is not clear in these studies. Using

results from an online survey and semi-structured interviews this chapter will explore the online experiences and behaviours of a sample of young adults in Ireland, Italy and the UK when they were between the ages of 12 and 16. Due to the sensitive nature of this topic, young adults between 18 and 25 were selected to participate. They were asked to retrospectively consider their behaviours and experiences of risk between the ages of 12 and 16 as adolescents are more at risk of being approached by online groomers than younger children (Quayle, 2010), predominantly as a result of age restrictions on SNS, although these are sometimes ignored by adolescents (Ball & Lilley, 2014).

From a developmental and cyber-psychological perspective, adolescence is a heightened time of risk online. As has been widely noted, due to the online disinhibition effect, people generally take more risks online than they do in real life (Suler, 2004). However, it must be noted that adolescents by their very nature are more likely to engage in risk-taking behaviour, thus being in the online environment, it is possible this disinhibition is exacerbated. Of particular concern is when a disinhibited adolescent comes into contact with a disinhibited sexual predator online. Research has indicated that those most at risk of online solicitations are girls and youth engaging in patterns of both offline (e.g. rule-breaking) and online risk-taking (e.g. interacting with strangers) (Livingstone et al., 2011; Quayle, Jonsson, & Lööf, 2012; Wolak, Finkelhor, Mitchell & Ybarra, 2008), such as children who are vulnerable, who are being bullied (Wolak Finkelhor & Mitchell, 2008) and/or who do not have good relationships/support systems with family/friends (Wolak, Finkelhor & Mitchell, 2003). Concerningly, online groomers have reported that markers of risk-taking encourage them to contact a young person (Webster et al., 2012). Groomers also seek out vulnerable youth who may be seeking to form bonds online – and their contact with such youth may be facilitated by the fast-track to intimacy afforded by the hyperpersonal communication effects (for further explanation of the hyperpersonal communication model see Nguyen, Bin & Campbell, 2012) of the internet (Walther, 1996).

Receipt of sexual solicitations by adolescents can be from an unwanted sender, or they can be part of a consensual dialogue (for example, from a partner). It is a normative function of adolescence to explore sexuality thus, it is not surprising this exploration might be conducted online. However, it should be noted that what forms part of a consensual dialogue between two young people can become problematic when shared beyond the intended recipient, for example a sext received and shared amongst friends, or revenge porn. Wolak and Finkelhor (2011) distinguish between two types of 'sexting'; that which is consensual and a normal part of experimentation is referred to as experimental sexting whereas the sharing of these

messages to an unintended audience or the involvement of an adult is referred to as aggravated sexting.

It is clear that the consequences of receiving sexual solicitations, such as a sexually explicit message online, will vary depending on the characteristics of the child, the sender and the context. Some children will be distressed (Finkelhor et al., 2000; Priebe, Mitchell and Finkelhor, 2013), some will take action to block or report (Webster et al., 2012; Priebe et al., 2013), some will ignore (Webster et al., 2012), and some will engage with the sender (Webster, et al., 2012). Some children may confide in others or report what has happened, however a significant amount of young people do not confide in parents or teachers for a number of reasons; they consider the behavior normal, they feel uncomfortable talking to parents, or they fear the removal of their electronic devices as a result of their parents finding out (Finkelhor et al, 2000; Webster et al., 2012; Priebe et al., 2013). The current project sought to explore this further and was therefore interested in whether young people who had received sexual solicitations had confided in or reported these sexual solicitations, and who they had confided to.

Understanding who children are likely to confide in when distressed about online sexual solicitation is vital as there has been limited research conducted in this area. As part of their research, Mitchell, Jones, Finkelhor, & Wolak (2013) examined youth's disclosure of online solicitation incidents and found that 53% of solicitations were disclosed to a trusted individual. Most participants disclosed information to a friend (37%) or parent/guardian (19%). Very few incidents were reported to a teacher or a higher authority such as law enforcement. Similar findings were reported by Livingstone et al. (2011) who reviewed risks and safety on the internet from the perspective of children across Europe. Their report found that 53% of those who had been bothered by sexual images they were exposed to online told someone about it. Regarding who children were most likely to confide in; 33% told a friend and 25% told a parent. These findings were comparable to Staksrud & Livingstone's (2009) study on children and online risk. Children in this study were much more likely to seek support from peers over parents and teachers after being exposed to inappropriate content or contact with individuals online. While research on who children are likely to disclose to with specific regard to online sexual solicitation is sparse, other research that examines negative online experiences in general report similar findings as the studies above. The EU Kids Online (2014) report examined children's (9-16 year-olds) online experiences across nine different countries in Europe. When discussing exposure to any type of risky content (including sexual content), younger children were inclined to be open to parental intervention whereas older children often spoke to peers for support. In another European wide study on mobile phone use amongst children and risks they

encounter online, Mascheroni & Cuman (2014) found that when young people reported negative online experiences they were most likely to seek support from mothers (71%), friends (57%) or fathers (54%). While communicative responses were found to be a way for young people to deal with negative online experiences, one in three children were unlikely to approach someone about this exposure. A lack of interest, not taking incidents serious enough and fear of punishment if they reported negative incidents are listed as motivations for children not to disclose their experiences with adults in this study.

There is some discussion in the literature regarding the importance of teaching young people how to navigate the internet safely and the role parents and educators should play in this respect. Research suggests that parents should maintain a dialogue with children regarding their activities online and create a safe space for young people to come forward and discuss uncomfortable and distressing situations without the fear of reprisal (e.g. confiscating their mobile telephones). It is clear from the literature that those who do not experience parental involvement such as monitoring and supervision are at heightened risk of experiencing online sexual exploitation (Wells & Mitchell, 2014; Webster et al., 2012; Wolak et al., 2008). Whilst most are in agreement that caregivers and educators alike should be involved in teaching young people about risk online, some research has identified that they may be ill-equipped to deal with this (Baker, 2010; Heslip, 2013; Ofcom, 2014). Equally, previous research has highlighted that whilst educational awareness programmes do improve the knowledge base of the students involved (Davidson & Martellozzo, 2008), young people may be unable to apply this knowledge to cyberspace and their lives online (Ofcom, 2014).

It is evident that whilst the internet provides important opportunities for young people, it also poses new risks to their well-being and safety. The internet offers favourable conditions for online sexual predators and it is important to conduct research to better understand the contact between young people and predators. It is hoped that results from the survey in this project of young adults across Ireland, Italy and the UK will provide a quantitative model for the construction of a typology of youth at risk for use by both law enforcement and industry. In addition, the information gathered on help seeking will provide important information for each country on encouraging young people to talk to others about getting sexual messages. Finally, the qualitative information presented offers an in-depth exploration of the experiences of those young adults who received online sexual messages as teenagers.

5.2 Descriptive findings

The total sample consisted of 1,166 respondents across three countries: England (n = 340), Ireland (n=529) and Italy (n = 297). The average age of the total sample was 21.23 years (*SD* = 2.15, range 18 - 25). The gender breakdown was disproportionate in the three countries, but the majority were females (Ireland: female = 344, male = 185; Italy: female = 222, male = 75 and England: female = 271, male = 69) (Φ = .14, p = <.001). The majority of participants were in education (n = 817, 70%), followed by employment (n = 265, 23%), unemployment (n = 64, 5%) and a small group who did not study or work (n = 20, 2%). Concerning ethnic background, we report on the two largest ethnic groups in each country, with smaller ethnic and/or culture groups amalgamated in the category 'others'. In Ireland, the largest ethnic groups were white Irish (n = 435, 82%) and any other white background (n = 53, 10%) (other = 8%); in Italy, the largest groups were south European (n = 271, 91%) and central European (n = 11, 4%) (other = 4%) and in England, white British (n = 135, 40%) and any other white background (n = 67, 20%) (other = 40%). More than 50% of the UK participants, 39% of the Italian and 33% of the Irish participants lived in a big city when they were teenagers and 28% of the Irish participants and less than one percent of the Italian and UK participants lived in rural areas.

In terms of sexual orientation, 77% (n = 406) of the participants living in Ireland defined themselves as heterosexual, 9% (n = 45) as gay or lesbian, 8% as bisexual (n = 44), 4% (n = 22) were unsure about their sexual orientation and 2% described themselves as 'other', which included asexual, pansexual and queer. Most respondents from Italy defined themselves as heterosexual (n = 269, 91%), three percent (n = 8) were gay or lesbian, four percent (n = 12) bisexual, two percent (n = 6) were unsure and 1% referred to themselves as 'other'. The majority of the respondents in the UK described themselves as heterosexual (n = 296, 88%), 5% (n = 13) as gay or lesbian, 4 percent (n = 12) were bisexual, 3 percent (n = 6) were unsure about their sexual orientation and 2% described themselves as 'other', which included asexual, pansexual and queer.

Internet use between the ages of 12 and 16

This section provides an overview of the amount of time participants spent online and the activities young people reported using the internet for between the ages of 12-16. How often respondents participated in each of the reported behaviours was also discussed. Findings are shown in table 8. Six percent of the sample went on the internet every hour when they were between the ages of 12-16 (n=68). Twenty-three percent went online every few hours (n=267) and 47% went online every day or almost every day (n=542). One fifth of the sample used the internet once or twice a week (n=231), 4% used it once or twice a month (n=41) and 2% used it a few times

a year (n=17). UK respondents were online significantly more frequently than both Irish and Italian respondents, and Irish respondents were online significantly more frequently than Italian respondents (Phi varies between .16 - .25, $p < .001$). There were no significant differences between how often males and females went online.

Listening to music, instant messaging, visiting social network sites and watching videos/movies were the four activities that were most often reported by the respondents. Participants less often visited chat rooms or virtual reality environments. Irish respondents reported significantly less involvement in playing games, chat rooms, listening to music, watching videos/movies and virtual worlds at age 12-16 compared to their Italian and UK peers (Phi varies between .16 - .56, $p < .001$). Italian respondents reported significantly less involvement in emailing, social network sites, instant messages and doing schoolwork (Phi varies between .13 - .26, $p < .01$).

Boys and girls significantly differed in their activity online, with the exception of emailing, going to chat rooms and watching videos/movies. Girls more often visited social networking sites (M = 1.67, SD = 1.67 for female and M = 1.86, SD = 1.05 for male, t (532) = -2.91, p = .005, 95% CI [-.322, -.062]); instant messaged (M = 1.60, SD = .91 for female and M = 1.76, SD = 1,00 for male, t (547) = -2.52, p = .001, 95% CI [-.287 .035]) than boys; were more likely to use an e-learning platform (M = 2.04, SD = .88 for female and M = 2.48, SD = .92 for male, t (573) = -7.44, p = .001, 95% CI [-.558, -.325]), and more often listened to music online (M = 1.50, SD = .77 for female and M = 1.70, SD = .89 for male, t (531) = -3.54, p = .001, 95% CI [-.088, -.308]) than boys. Boys significantly more often played online games (M = 1.70, SD = .88 for female and M = 2.06, SD = .95 for male, t (647) = 2.63, p = .001, 95% CI [.254, .484]), and had significantly more experience with virtual worlds than girls (M = 3.19, SD = .97 for female and M = 2.98, SD = 1.15 for male, t (516) = 2.91, p = .001, 95% CI [.068, .35]).

***Table G**. Descriptive statistics of internet activities*

Internet activities	Often	Sometimes	Rarely	Never	Total
	N %	N %	N %	N %	N %
E-mailing	71 (6)	287 (26)	457 (40)	321 (28)	1146 (100)
Social network sites	642 (55)	295 (25)	127 (11)	96 (8)	1160 (100)
Instant messages	694 (60)	275 (24)	94 (8)	95 (8)	1158 (100)
Playing games	443 (38)	417 (36)	205 (18)	96 (8)	1161 (100)
Chat rooms	247 (22)	223 (19)	251 (22)	423 (37)	1144 (100)
Doing schoolwork	305 (26)	463 (40)	296 (25)	98 (8)	1162 (100)
Virtual worlds	108 (9)	214 (19)	244 (21)	585 (51)	1151 (100)
Listening to music	704 (61)	317 (27)	93 (8)	49 (4)	1163 (100)
Watching videos/movies	501 (43)	357 (31)	190 (16)	115 (9)	1163 (100)

Note. N = Number of participants

Respondents were most likely to access the internet using their mobile phones (used by 90%), and desktop computers (80%), while around half accessed the internet using a gaming console (52%) or laptop (49%). A minority of 8% of respondents used a tablet to access the internet. Girls used mobile phones significantly more often than boys (M = 1.09, SD = .28 for female and M = 1.14, SD = .35 for male, t (503) = -2.41, p = .016, 95% CI [-.094, .10]); and boys were significantly more likely to use gaming consoles than girls (M = 1.57, SD = .50 for female and M = 1.25, SD = .43 for male, t (674) = 10.09, p = .001, 95% CI [.254, .377]). The use of all five of the devices was significantly lower in Italy compared to Ireland and England (Phi varies between .12 - .29, $p < .001$).

Parental monitoring

Respondents were asked how often their parents asked them about their online activity when they were between the ages of 12-16. Twenty-six percent of the parents 'often' asked what they doing and 34% 'sometimes' were asked about their behaviour on the internet. Twenty-six percent 'rarely' and 14% 'never' asked questions about what they were doing on the internet. Almost 65% of the respondents were convinced that their parents had 'never' blocked or filtered their Internet access, 21% didn't know and 14% reported that their parents took some

security measures on the internet. Compared to Ireland and Italy, the parents of the UK respondents were significantly more likely to control their youth's Internet access by blocking or filtering ($\Phi = .17$, $p < .001$).

Relationships, school, and neighbourhood

Respondents were asked how true they felt the following statements were about their lives between the ages of 12 and 16: "I had at least one good friend I could rely on", "I lived in a neighbourhood where it was safe to go out alone in the dark", "I got on well with my parents" and "I mostly enjoyed being in school". Rates are shown in table 9. The majority of 64% of respondents felt it was certainly true that they had at least one good friend they could rely on when they were teenagers. Approximately half of respondents felt it was certainly true that they lived in a safe neighbourhood, and that they got on well with their parents. A lower proportion of 37% of respondents reported that it was certainly true that they mostly enjoyed being in school between the ages of 12 and 16.

Girls were more likely to answer that they had a good friend to rely on and that they mostly enjoyed school ($M = 2.60$, $SD = .59$ for female and $M = 2.51$, $SD = .65$ for male, t (1162) = 2.21, $p = .027$, 95% CI [.010, .172] and $M = 2.21$, $SD = .73$ for female and $M = 2.05$, $SD = .77$ for male, t (1164) = 3.37, $p = .001$, 95% CI [.068, .256], respectively). On the other hand, boys were more likely to feel that they lived in a neighbourhood where it was safe to go out after dark ($M = 2.30$, $SD = .70$ for female and $M = 2.52$, $SD = .68$ for male, t (1164) = -4.83, $p = .001$, 95% CI [.-.310, .-.132]. Irish and UK youth responded more positively to the items on friends, parents and school than Italian youth (Phi ranged from .104 to .306, $p<.05$). Irish respondents also rated the safety of their neighbourhood more positively than both UK and Italian respondents (Phi ranged from .130 .183, $p<.001$).

***Table H**. Descriptive statistics on lifestyle factors*

Statement	Not True	Somewhat True	Certainly True	Total
	N %	N %	N %	N %
I had at least one good friend I could rely on	74 (6)	342 (29)	748 (64)	1164 (100)
I lived in a neighborhood where it was safe to go out alone in the dark	153 (13)	439 (38)	574 (49)	1166 (100)
I got on well with my parents	130 (11)	419 (36)	614 (53)	1163 (100)
I mostly enjoyed being in school	239 (21)	496 (43)	431 (37)	1166 (100)
Note. N = Number of participants				

This section begins by providing an overview of the problematic offline behaviours respondents engaged in when they were between the ages of 12 and 16. A description of risky behaviours young people engaged in online is then provided. The frequency at which respondents received online sexual solicitations is then presented, followed by an insight into whom the respondents were invited to engage in sexual activities with on the internet.

Problematic offline behaviour between ages 12-16

Participants were asked how often they engaged in problematic, or risky behaviour offline when they were between the ages of 12 and 16. Table I indicates that just over half of the respondents never had so much alcohol they got really drunk, or played truant from school, or got in trouble with teachers for bad behaviour. Less than 10% and 20% of the respondents reported 'often' and 'sometimes' respectively on these three items. Therefore, the majority of the sample was not regularly involved in problem behaviour as mentioned in Table 3. More than 80% 'never' used drugs and only 2% reported to have used drugs 'often' between the ages of 12 to 16 years.

With the exception of alcohol consumption, males reported significantly more problem behaviour offline compared to female respondents ('played truant from school': M = 3.33, SD = .90 for female and M = 3.19, SD = .98 for male, t (1163) = 2.33, p = .02, 95% CI [.023, .268]; 'got in trouble with teachers for bad behaviour': M = 3.39, SD = .88 for female and M = 3.03, SD = .99 for male, t (1163) = 5.95, p = .001, 95% CI [.237, .469] and 'used drugs': M = 3.74, SD = .66 for female and M = 3.52, SD = .85 for male, t (1164) = 4.18, p = .001, 95% CI [.115, .320]). Italian respondents reported playing truant from school significantly more often than UK and Irish respondents, and they reported getting into trouble for bad behaviour significantly less often (Phi varies between .12 - .17, p < .01).

***Table I**. Descriptive statistics for risky offline behaviour*

Problematic behaviour offline	**Often**	**Sometimes**	**Rarely**	**Never**	**Total**
	N %	N %	N %	N %	N %
Had so much alcohol I got really drunk	92 (8)	206 (18)	244 (21)	624 (53)	1166 (100)
Played truant from school	70 (6)	168 (14)	278 (24)	649 (56)	1166 (100)
Got in trouble with my teachers for bad behaviour	82 (7)	133 (11)	319 (27)	631 (54)	1165 (100)
Used drugs	27 (2)	98 (8)	101 (9)	940 (81)	1166 (100)

Note. N = Number of participants

Risky behaviour online

Participants were asked about how often they engaged in risky activities related to the internet. Without exception, all respondents were found to have engaged in some form of risky online behaviour. Five activities were more pronounced than others and achieved higher risk scores (see Table J). These five risky activities were: downloading pirated material such as games, music and illegal films (often & sometimes = 58%), sharing photos/videos (often & sometimes = 59%), adding or accepting people online without ever meeting them before (often & sometimes = 47%), posting personal information online (often & sometimes = 36%) and visiting adult pornographic sites (often & sometimes = 27%). Meeting an unknown peer face to face did not occur very often (often & sometimes = 14%); and meeting an unknown adult face to face occurred very rarely (often & sometimes = 3%).

***Table J**. Descriptive statistics of risk behaviour on the internet*

Risk behaviour online	Often	Sometimes	Rarely	Never	Total
	N %	N %	N %	N %	N %
Gave personal information online	104 (9)	319 (27)	389 (34)	344 (30)	1156 (100)
Downloaded pirated material	321 (28)	350 (30)	193 (17)	291 (25)	1155 (100)
Added or accepted people online without ever meeting them	200 (17)	345 (30)	280 (24)	330 (29)	1155 (100)
Visited adult pornographic sites	121 (11)	189 (16)	171 (15)	675 (58)	1156 (100)
Shared photos/videos	293 (25)	395 (34)	254 (22)	211 (18)	1153 (100)
Met a peer face to face you only knew online	46 (4)	117 (10)	192 (17)	800 (69)	1155 (100)
Met an adult face to face you only knew online	12 (1)	17 (2)	41 (3)	1085 (94)	1155 (100)

Note. N = Number of participants

The results suggest that boys engaged in more risk taking behaviour on the internet than girls, with the exception of sharing photos/videos online, which girls did significantly more often (M = 2.25, SD = 1.05 for female and M = 2.53, SD = 1.02 for male, t (603) = -4.05, p = .001, 95% CI [-.410, -.143]). Boys were significantly more engaged in the following activities than girls: downloading pirated material (M = 2.47, SD = 1.13 for female and M = 2.21, SD = 1.14 for male, t (597) = 3.49, p = .001, 95% CI [.113, .404]), visiting adult pornographic sites online (M = 3.62, SD = .74 for female

and *M* = 2.17, *SD* = 1.03 for male, *t* (465) = 23.27, *p* = .001, 95% CI [1.331, 1.577]), and meeting an adult face to face they had only met online (*M* = 3.93, *SD* = .36 for female and *M* = 3.85, *SD* = .55 for male, *t* (437) = 2.42, *p* = .005, 95% CI [.026, .134]) . There were some country-specific differences. Fewer UK respondents stored personal information on the Internet (Φ = .13, p < 0.005); less Irish respondents added/accepted people as friends they had never met face to face (Φ = .14, p < .005), and more Irish respondents visited adult pornographic sites at age 12-16 (Φ = .15, p < .001).

Harassment experience

Participants were asked how often they had been harassed or threatened online or face to face, and how often they had ever harassed or threatened someone else online or face to face. Table K indicates that 17% ('often' & 'sometimes') reported being harassed/threatened online or by text while 19% indicated that they 'often' or 'sometimes' had to deal with this offense face to face when they were between 12-16 years old. Four percent of respondents reported to have harassed/threatened others between the ages of 12-16 online or by text, and the same percent reporting doing this face to face. The large majority of around 85% of respondents had never harassed or threatened someone else online of offline.

***Table K**. Experiencing and perpetrating harassment on and offline*

	Often	**Sometimes**	**Rarely**	**Never**	**Total**
	N %	N %	N %	N %	N %
Being harassed/threatened online by text	38 (3)	157 (14)	257 (22)	704 (61)	1156 (100)
Being harassed/threatened face to face	58 (5)	156 (14)	263 (23)	679 (58)	1156 (100)
Harassed/threatened someone online	6 (1)	38 (3)	138 (12)	974 (84)	1156 (100)
Harassed/threatened someone face to face	10 (1)	32 (3)	132 (11)	982 (85)	1156 (100)

Note. N = Number of participants

Boys were significantly more often harassed/threatened face to face than girls were (*M* = 3.45, *SD* = .85 for female and *M* = 3.10, *SD* = .96 for male, *t* (534) = 5.83, *p* = .001, 95% CI [.235, .474]). However, boys engaged in such behaviour significantly more often than girls (*M* = 3.85, *SD* = .45 for female and *M* = 3.69, *SD* = .64 for male,

t (460) = 4.10, *p* = .001, 95% CI [.082, .234]). Boys significantly more often harassed/threatened someone else online by text (*M* = 3.85, *SD* = .46 for female and *M* = 3.67, *SD* = .60 for male, *t* (479) = 4.90, *p* = .001, 95% CI [.108, .253]). Fewer respondents from Italy reported being a victim of harassment and/or threatening behaviour in the past than the other respondents (Φ = .28, p < .001). Italian respondents also reported that they threatened/harassed others via the Internet by text the least out of all countries examined (Φ = .17, p < .001).

Sexting

This section addresses the question of whether the respondents had sent sexually suggestive messages (sexting) via smartphone, text, video or film in the past (between 12-16 years), to known or unknown people. In general, these activities did not happen often. Almost 9% of respondents send a sext to someone they only knew online (n = 100); 18% to a boyfriend/girlfriend (n = 201), 6% to a friend/acquaintance from school (n = 69), 5% to a friend/acquaintance from somewhere else (n = 52), 9% to someone else they were romantically interested in (n = 100), and 4% to someone they didn't know (n = 46). Despite these findings, sexting was rare in the research and there were some gender differences. Generally, boys were more often engaged in sexting than girls were in the following three scenarios: boys sent significantly more suggestive sexual messages to someone they only know online (*M* = .07, *SD* = .26 for female and *M* = .12, *SD* = .33 for male, *t* (491) = -2.30, *p* = .05, 95% CI [-.087, -.007]); to friends/acquaintance from school (*M* = .05, *SD* = .22 for female and *M* = .09, *SD* = .28 for male, *t* (478) = -2.12, *p* = .05, 95% CI [-.071, -.003]), and to someone else they were romantically interested in (*M* = .07, *SD* = .26 for female and *M* = .12, *SD* = .33 for male, *t* (484) = -2.49, *p* = .05, 95% CI [.088, -.015]).

Frequency of receiving sexual solicitations online

This section focuses on how often respondents were invited by others to engage in sexual behaviour on the internet. Table L indicates that the vast majority of respondents 'never' had to deal with such sexually explicit online requests. However, a significant minority did receive such requests 'often' or 'sometimes', when they were between 12 and 16 years old. In general, girls were significantly more likely to be invited to engage in sexual behaviour on the internet than boys were. This applies to three of the four activities in Table 6. Girls were more often invited to post sexual information about themselves on the internet (*M* = 3.24, *SD* = .95 for female and *M* = 3.45, *SD* = .84 for male, *t* (668) = -3.56, *p* = .001, 95% CI [-.316, -.092]), to do something sexual online (*M* = 3.49, *SD* = .83 for female and *M* = 3.60, *SD* = .75 for male, *t* (655) = -2.25, *p* = .05, 95% CI [-.215, -.015]), and to post sexually suggestive photo's/videos of themselves on the internet (*M* = 3.38, *SD* = .92 for female and *M* = 3.60, *SD* = .74 for male, *t* (699) = -4.188, *p* = .001, 95% CI [-.329, -.119]).

***Table L**. Being invited to act sexually online*

Invited to act sexually online	Often	Sometimes	Rarely	Never	Total
	N %	N %	N %	N %	N %
Ask for sexual information about yourself	51 (4)	213 (19)	220 (19)	658 (58)	1142 (100)
Ask to do something sexual	36 (3)	127 (11)	185 (16)	794 (70)	1142 (100)
Ask for a sexually photo/video of yourself	51 (4)	151 (13)	185 (16)	755 (66)	1142 (100)
Meet up to engage in sexual activities	23 (2)	78 (7)	137 (12)	903 (79)	1141 (100)
Note. N = Number of participants					

The percentage of youths that had *ever* been sexually solicited was calculated and it was found that 44% (n=233) of respondents in Ireland, 53% (n=181) of respondents in the UK and 39% (n=116) of respondents in Italy had been sexually solicited online between the ages of 12 and 16. The UK sample was significantly more likely to have been sexually solicited online. No difference between Ireland and Italy was found. (Phi ranging 0.09-0.14, p< .01).

Identifying senders of sexual solicitation

Next, respondents were asked who they had received online sexual solicitations from. Nineteen percent (n = 214) were solicited by someone they only met online, 16% (n = 183) were solicited by a boyfriend/girlfriend at that time, 8% (n = 93) by a friend/acquaintance from school, 9% (n = 104) by a friend/acquaintance from somewhere else, 12% (n = 140) by someone else the respondents were interested in, 6% (n = 71) by someone else they knew, 15% (n = 169) by an unknown person and in 3% (n = 29) the origin of the solicitor was not clear. Only one type differed significantly between boys and girls. Girls were significantly more often solicited by a person they didn't know (*M* = .18, *SD* = .38 for female and *M* = .08, *SD* = .27 for male, *t* (827) = 4.93, *p* = .001, 95% CI [.053, -.145]).

Age and gender of those sending sexual solicitation

According to the respondents, 26% of them (n = 290) had received solicitations from someone around the same age as they were at that time (12-16 years), 10% (n = 111) received solicitations from someone five or more years older and 15% (n = 176) reported that they'd received solicitations from someone one to four years older. Only 2% (n = 26) had received solicitations from someone younger, and 5% (n = 57) of respondents reported that the age of solicitor was unknown. Gender-differences

were not examined for solicitors who were younger than the respondents in the research group and for unknown persons because of too few respondents. Girls were significantly more often approached by older solicitors than boys: for five years or older (*M* = .11, *SD* = .32 for female and *M* = .06, *SD* = .23 for male, *t* (803) = 3.42, *p* = .001, 95% CI[.025, -.092]), and one to four years older (*M* = .18, *SD* = .39 for female and *M* = .08, *SD* = .28 for male, *t* (810) = 4.80, *p* = .001, 95% CI [.059, -.140]). Boys were significantly more often approached by peers (*M* = .24, *SD* = .43 for female and *M* = .31, *SD* = .46 for male, *t* (546) = -2.32, *p* = .05, 95% CI [-.128, -.011]).

5.3 Inferential findings

Profiles of Youth

Cluster analysis was used to identify profiles in the young people. This involved combining k-means and hierarchical cluster analysis techniques to explore whether the participants could be grouped into profiles on the basis of the variables measured. Four profiles were identified and are described below.

The Adapted Adolescent (n=503) was the least likely to engage in on and offline risk, least likely to be harassed, and one of the least likely to receive sexual solicitations. This was the largest single group of participants across the investigation. There is no significant aggression to others either in cyberspace or in the real world, few report requests for sexual information about themselves from partners, strangers or unknown adults. Whilst they demonstrate a slight increase in sharing and posting videos online; these videos are not identified as being specifically of a sexual nature and are more likely linked to their engagement on social media sites such as Instagram, Facebook and Twitter.

Inquisitive non-sexual (n=280) were predominantly male and have lower risk taking offline but higher online risk-taking. They are the least likely, along with the adapted adolescent, to receive sexual solicitations, or send sexts. They were likely to engage in risky online behaviour linked to the sharing of information with strangers; downloading virus's and other questionable material; visiting adult pornographic websites; accepting strangers as friends; and downloading illegal material (i.e. music, videos). Their sexual engagement from 'real' individuals, as already mentioned, is limited however they do view adult pornography.

The Risk-taking Aggressive Adolescent (n=84) was the highest risk taking on and offline, most likely to both harass and be harassed, most likely to receive solicitations and one of the most likely to send sexts. They demonstrated a pattern of real world anti-social behaviour such as problems with authority (parents and

teachers), truancy, school exclusion, drug and alcohol use. In addition, this group is defined by the highest levels of online/offline aggression towards others, together with a heightened level of experiencing online/offline victimisation at the hands of others. This group appears to act more aggressively towards their peers in both the real and virtual worlds, which is reflected in their self-report of more frequent harassment of others both face to face and online.

Inquisitive sexual (n=225) comprised mostly of females, and demonstrated very similar patterns of risks and behaviours to the inquisitive non-sexual. They watched less pornography but were more likely to receive sexual solicitations and send sexts. They show the highest scores across all profiles in receiving requests for sexual information both general and specific and also demonstrate high likelihood of meeting up to engage in a sexual activity.

Profiles at risk of sexual solicitation by adults

Sexual solicitation is defined by the participants receiving an online sexual solicitation from someone at least 5 years older when they were 12-16 years old. Of those who had received sexual solicitations (n=530), 21% of these (n=111) had been from an adult. At the lower risk end, this would involve for example a 12 year old receiving a sexual request from someone at least 17 years old. A series of logistic regression analyses were conducted to examine the likelihood of each profile having received sexual solicitations from adults (see table M).

Logistic regression analyses indicated that the risk-taking aggressive youth profile were significantly more at risk of receiving sexual solicitations from adults than the other three profiles. The odds of these youths receiving an online sexual solicitation from an adult were 34 times higher than the adapted adolescent, 15 times higher than the inquisitive non-sexual profile and twice as high as the inquisitive sexual group. The inquisitive sexual group group were the second most likely group to receive sexual solicitations from adults – they had 14 times the odds of receiving an online sexual solicitation from an adult compared to the adapted adolescents, and 6 times the odds of the inquisitive non-sexual group. There were no significant differences between the adapted adolescent and the inquisitive non-sexual group in terms of their likelihood of receiving sexual solicitations.

Table M. Profile comparison of risk for online sexual solicitation by an adult

Reference Group		B	S.E.	Odds Ratio
Adapted Profile	Inquisitive non-sexual	0.79	0.44	2.20
	Inquisitive sexual	2.65***	0.36	14.09
	Risk-taking aggressive	3.51***	0.39	33.52
Inquisitive non-sexual	Inquisitive sexual	1.85***		
	Risk-taking aggressive	2.72***		
Inquisitive sexual	Risk-takings aggressive	0.87**	0.27	2.38

Vulnerabilities & risk behaviours associated with online sexual solicitation by an adult

This project was also interested in the relation between different types of vulnerability and risk factors associated with the likelihood of youth receiving sexual solicitations from adults. The factors considered included the following:

- Vulnerabilities: being female, being of a minority sexual orientation, not having a good friend to rely on, not having a good relationship with parents, living in an unsafe neighbourhood, not enjoying school, being bullied on or offline.
- Lack of monitoring or internet education: parents putting no blocks or filters on internet use, parents not asking about online activity, no internet education;
- Risky offline behaviours: getting drunk, skipping school, getting in trouble at school and taking drugs.
- Risky online behaviours: sharing personal information online, accepting/adding unknown people to their friends list, downloading pirated material, sharing photos/videos online, bullying others online, viewing adult pornography, meeting an unknown peer offline, meeting an unknown adult offline, sexting as a teenager.

Correlational analyses were first conducted to identify significant associations between each variable and the likelihood of receiving a sexual solicitation from an adult. The majority of relationships demonstrated significant relationships. However, the following variables were **not** significantly associated with the likelihood of being sexually solicited by an adult: not having a good friend to rely on, not having a good relationship with parents, living in an unsafe neighbourhood, parents putting no blocks or filters on internet use, parents not asking about online activity, no internet education and taking drugs.

Using the variables significantly correlated, a logistic regression was conducted to examine which of these factors uniquely predicted the likelihood of receiving a sexual solicitation from an adult. Only a few variables remained uniquely significant. Table N indicates that controlling for all other vulnerabilities and risk factors, girls had 5 times the odds of being sexually solicited by an adult. Youth who were more frequently harassed or threatened (on or offline) were more likely to be sexually solicited online, as were those who more often added/accepted unknown people to their friends lists. Those who were less likely to harass or threaten others online were also the youth at increased risk. Finally, youth who more frequently watched adult pornography as teenagers, and who sent someone else a sexual message or request, had increased odds of being sexually solicited by an adult.

Table N. Logistic regression analysis –risks and vulnerabilities for online sexual solicitation by an adult (outcome variable)

Category of risk	Variable	B	S.E.	Odds Ratio
Vulnerabilities	Female	1.62***	0.36	5.06
	Not heterosexual	0.49	0.27	1.63
	Does not like school	0.11	0.27	1.12
	Frequency of being harassed/threatened offline or online	0.54***	0.15	1.71
Risky offline behaviours	Frequency of alcohol consumption to get drunk	0.15	0.12	1.17
	Frequency of skipping school	0.03	0.13	1.03
	Frequency of harassing/threatening others offline	0.10	0.24	1.10
Risky online-related behaviours	Frequency of sharing personal information online	0.01	0.13	1.01
	Frequency of downloading illegal material	0.04	0.12	1.04
	Frequency of accepting unknown people to friends list	0.43**	0.13	1.54
	Frequency of sharing photos/videos online	0.01	0.13	1.01
	Frequency of harassing/threatening others online or by text	-0.57*	0.26	0.57
	Frequency of viewing adult pornography	0.33*	0.14	1.39
	Frequency of meeting unknown peer offline	-0.21	0.15	0.81
	Frequency of meeting unknown adult offline	0.39	0.23	1.48
	Sent sext as a teenager	0.94***	0.24	2.57

***p<.001 **p<.01 * p<.05

Formal and informal help-seeking behaviour

In general, of the 509 respondents who received online sexual messages and requests in between the ages of 12-16, 54% (n = 276) talked to someone about the experience. Respondents in the UK were significantly more likely to talk to someone than respondents in Ireland and Italy, with respondents in Italy more likely to talk to someone than those in Ireland (Phi varies between .12 - .52 $p < .05$). Formal help-seeking behaviour was reported in only a handful of cases, while informal help-seeking behaviour took place more often. Talking to someone about receiving sexual messages or requests over the internet was mainly done with friends and to a much lesser extent, with parents, a boyfriend/girlfriend or someone else.

***Table** O. Rates of Informal and formal help-seeking behavior*

Informal help-seeking behaviour				**Formal help-seeking behaviour**			
Question asked	Yes	No	Total	Question asked	Yes	No	Total
	N %	N %	N %		N %	N %	N %
I told my mother or father	27 (4)	568 (96)	595 (100)	**I called a helpline**	1 (0)	589 (100)	600 (100)
I told my brother or sister	18 (3)	574 (97)	592 (100)	**I told a teacher**	3 (1)	587 (99)	590 (100)
I told a friend	218 (33)	446 (67)	664 (100)	**I told someone whose job it is to help (i.e., police, social worker)**	7 (1)	586 (99)	593 (100)
I told my boyfriend/girlfriend at that time	42 (7)	558 (93)	600 (100)	**I used an online reporting mechanism**	13 (2)	579 (98)	592 (100)
I told another adult I trust	5 (1)	584 (99)	589 (100)				
I told someone else	26 (4)	564 (96)	590 (100)				
Note. N = Number of participants							

In the next section these issues are explored in depth interviews with a subset of the young people.

Qualitative analysis of depth interviews

The objective of this analysis was to explore young people's perceptions of their online interactions, learnings and recommendations for online safety. Participants were asked to recollect how they behaved online when they were younger through semi-structured interviews. The methodology can be found earlier in this report at page 24.

The thematic analysis identified 8 themes:

1. *Risk-taking behaviour online*

2. Role of parents in child's online world

3. The importance of Identity and social status on self-esteem

4. Online safety education & knowledge

5. Exposure to inappropriate/upsetting content online

6. Positive aspects of the Internet

7. Role of key stakeholders

8. Advice to young people today.

These themes provide help to provide a structured understanding of young people's experiences of online interactions.

Risk-taking behaviour online

Analysis revealed that risky online behaviours were common place among participants and that they engaged in similar types of behaviours across the data set regardless of nationality. Behaviours ranged from low risk inquisitive behaviours (such as downloading pirated material which results in inadvertently downloading viruses) to aggressive high risk taking, such as engaging in sexual activity live through web cams or streaming services. Communication with strangers online via social media, chatrooms or online games was often cited as being the main risk participants felt they took online. This type of communication tended to begin when participants received friend requests or unsolicited messages from strangers accounts. At an earlier age, participants did not seem to understand the risk of accepting such requests. Many social media platforms allow strangers to contact youth directly.

'…Actually when I talked to strangers it was mostly because they contacted me…'

(UK1, 2016)

Communication with strangers seemed to have been a catalyst for young people to engage in risky behaviours such as disclosing personal information.

'…as I said before, I remark that ten years ago I had some potentially risky behaviours, surely risky, perhaps I would give sensitive data to people...'

(ITA3, 2016)

Meeting up with strangers met online, in real life, was a major problem the group engaged with. With hindsight the risk involved is acknowledged. The participants were cognisant of the fact that you due to online anonymity, there is a danger that the person they go to meet may not be who they said they were online. While the majority of people ended up meeting people their own age, they were aware that the person they were meeting is could have been anyone. While none of the sample interviewed experienced negative consequences from meeting a stranger offline, it was common place amongst their peers to would meet strangers.

'…Yeah, yeah but a lot of my friends actually met people that you know…they would go to the mall and the guy is not there, or maybe the guy is there but it is not the guy they are looking for…'

(IRE2, 2016)

Posting public photos of themselves on various social media was discussed in terms of risk as any stranger would have access to their image and could do anything they wanted with them. Public images are universally accessible and therefore can be used by anyone on any site whether for innocent or nefarious reasons. This was a risk that many teens were not cognitive of at the time of posting:

'…I have always tried to be careful, but maybe I don't know, when I was younger maybe, I didn't know the risks that well. Maybe you post a photo which is public so everyone can see it. Maybe that was the riskiest…'

(ITA4, 2016)

Conversations with strangers often lead to a request for the youth to send pictures of them, which was generally met with suspicion from participants.

'…I think it's dangerous, you don't know who you are talking to, maybe you think you are talking to a person but you are talking to another one and I do think that online we feel safe (unintelligible) you feel like you're not exposing yourself and you actually are…'

(IRE2, 2016)

Participants discussed the negative consequences that can occur from online sexual risk-taking. While nobody claimed they had suffered consequences, many had experienced negativity vicariously through peers. Revenge porn emerged as a modern form of exploitation that many of the sample had friends experience:

'…Pretty much everyone I know has a friend who knows someone who has had their pictures leaked online. So everyone is like kind of more careful with it and they had conversations leaked, like they are talking about sex or something…'

(IRE2, 2016)

The longevity of posting online emerged as an issue. Participants were young at the time of posting; naivety played a large role in driving youths to risk taking behaviours. Communicating with strangers or posting pictures of themselves was not seen as an activity that could have consequences:

'…you don't think that the internet is such a vast platform that truly anyone in the world can see it…'

(ITA4, 2016)

Drivers leading youth to engage in risk taking behaviours emerged relating to boredom. This boredom mixed with teenage impulsivity combined for engaging in risky behaviour.

'…I don't know, I was really curious about it and then once someone told me, oh you can do this, it's risky but you can do it, I told all my friends about it and it became like kind of a hype, like it's dangerous but it's cool and we want to do it…'

(IRE2, 2016)

Owning or possessing personal ICT devices and having private space to use technology were also considered a catalyst to risk taking behaviour. These heightened the chances of participants engaging in risky behaviour in the absence of typical parental or caregiver supervision and monitoring. Peers tended to use friends whose internet use was not supervised as a catalyst for them to engage in behaviours or view content they would not be allowed to do in their own home.

'…I would rather watch them with a friend of mine whose parents were more inclined to let him do what he pleased…'

(ITA3, 2016)

Friends influence each other to take risks and there is an element of peer acceptance and striving to be accepted. Youth seem to be influenced by their friends when deciding on how to act and where to go online. For example, there are signs that youths get involved in sexting because '*...everybody does that…*' and that for young people it has '*become their normality*…'. One participant expressed regrets about this behaviour:

'…I wish I did not have that freedom. It's... It's like I did not have so much control over a lot of things and, wish I wasn't with my friends when they went to [Website]…'

(UK1, 2016)

Exposure to inappropriate online material

When describing the negative content exposed to online, participants described receiving significant numbers of unwanted messages from older male strangers who were '*Mainly teenagers, but there were adults too*…'. Some of these messages made the participants uncomfortable upon receipt.

> *'…Many people, especially many older boys, sent messages and they were annoying, too, and worrying…'*
>
> **(ITA3, 2016)**

Many of the messages contained sexually explicit content: '*Their messages were, I'd say, too sexual*…'. This content could manifest itself as pornography, explicit videos, images and texts from people they are communicating with online.

> *'… some people who liked to act weird over you and ask you to do something like sexual hints, as well as to my friend, but I would never have it on purpose…'*
>
> **(UK1, 2016)**

Participants described how their normal everyday online experience can be hijacked by people who keep trying to engage in sexual behaviour or conversations, even on sites that have nothing to do with sex.

> *'…We went there for fun, but soon as you're on it, people can private message to you and the people private messaging you aren't talking about the topic, but about sex. They all are interested in you to undress…'*
>
> **(UK2, 2016)**

Exposure to sexual content led to many of the participants experiencing negative emotions as in the main, the material and experiences were ones that they did not want to be introduced to. Participants expressed fear and that the content made them feel '*uncomfortable*':

> *'…It made me learn about people, and know about things that I didn't know about. But in a bad way. I didn't want to know that, be in that, or seeing that, or being in that situation…'*
>
> **(UK2, 2016)**

> *'…saw a guy and he took off his underwear and it was not something I needed to see at that time, cause it kind of scared me and I thought it was weird and I don't like that…'*
>
> **(IRE2, 2016)**

Exposure to sexual content did lead to many participants changing how they behaved online and who they trusted. Some felt it was difficult to trust anybody they met online after having negative interactions or experiences.

> *'…When I was a teenager I spent lot of time online and I would have liked to talk with strangers but now I'm not that willing to…it made me feel less curious, and less interested in boys, all these sexual messages. I wouldn't know who was the good one or who could be mean to me…'*

(UK1, 2016)

Online safety education and knowledge

Overall participants involved believed that their knowledge of online safety was '*limited*' when they first engrossed themselves into the online world.

> *'…I have always tried to be careful but maybe don't know, when I was younger maybe, I didn't know the risks that well…'*

(ITA4, 2016)

There was a feeling that the lack of knowledge young people had about online safety was a reason why they were likely to engage in risky behaviour. For instance, posting images online without any knowledge of data protection or terms and conditions of websites that might keep their data and images online well after individuals delete them.

> *'…Like if I had enough information like the pictures I post online won't ever be completely deleted like, I didn't know anything about cloud at the time and I obviously didn't know...'*

(IRE2, 2015)

Frustration was expressed about the lack of education in schools in particular. Many reported receiving no education about online safety and those that did receive online education at school reported that the content was not relevant when compared to what they are exposed to online.

> *'…A lot of the talks we would have gotten in primary school would have been quite out-of-date…you know…so…you know it just…they just weren't very good basically the information that we got…'*

(IRE1, 2015)

There was a sense of regret that the participants had not received better education or information about what actions to take when dealing with negative experiences and dangers. Interestingly, it was widely acknowledged that detailed specific education was

needed from visiting experts in security, cyberpsychology, policing or social media, rather than having teachers or parents telling them '*Don't do that*'.

> *'…if the exact same talk was delivered by a teacher I don't think it would have had as much as of effect as having an external person visit…'*
>
> **(IRE1, 2015)**

> *'…we called experts those people who came to school and talked about a topic they knew better than the professors…'*
>
> **(ITA3, 2016)**

Role of stakeholders

Other than schools there were suggestions that other stakeholders could do more to ensure child safety online. With regards to industry, there were complaints that safety procedures and report mechanisms were too complicated to follow and there were also a number of misconceptions about reporting inappropriate material which stopped individuals from acting. There is also a widespread belief that even if something is reported nothing will be done about it.

> *'…When something gets reported, something should actually be done... But it's like the community standards are very low. I think it could be very, very unsafe. I haven't found yet a social media that can be safe and that can't be harmful…'*
>
> **(UK2, 2015)**

After registering with certain social media sites, many profiles have low privacy settings until they are changed by the owner of the account. Many young people do not know this or underestimate the risks online and by not altering their settings.

> *'…I remember when I was on Facebook it was a year before I realised that friends of friends could see all my posts…I would have been properly nearly posting about everything…for under 18's it should be maximum privacy until you decide…'*
>
> **(IRE1, 2015)**

One area where it was believed industry should be more responsible is for who registers on their site. People must be a certain age in order to register for social networks sites and range of age vary depending on the content of the website. However, participants report having accessed websites for years that they were too young to be on as it is very simple to change your age when registering, thus increasing their availability and vulnerability to strangers.

> *'…even since I was 12 I always register my age as 18. I've been 18 for years…'*
>
> **(UK1, 2015)**

Participants tended to have pessimistic views on what the law enforcement can do to help them with any negative issues that occur online. There is a perception that because the majority of resources are used to fight serious offline crimes, there is little time left for online criminality. When they have gotten involved with issues, some jurisdictions don't seem to have sufficient expertise in online crime to help.

> *'...they just say there's nothing we can do that's kind of all I've heard from about four or five different people who I've known of going through something like that…'*
>
> **(IRE1, 2016)**

Role of parents in child's online world

The role of the parent in educating children about online safety is another well discussed topic. There has been debate about where responsibility lies with regards to teaching young people about the dangers of the internet. An issue that many participants had was that they felt their parents were not knowledgeable about the online world. Thus they were not seen as a credible or legitimate source of information. As online technology evolves, the knowledge gap between older generations and youths seems to widen.

> *'…I took advantage of my parents' lack of information, in the sense that while chatting I always said I was chatting with people I knew, though sometimes I did not know them…'*
>
> **(ITA3, 2016)**

> *'…their parents don't know what they are talking about then they are not going to listen to them anyways…'*
>
> **(IRE1, 2016)**

There were signs that those that received heavier internet monitoring were less likely to engage in high risk behaviour online. Most participants reported some level of risk taking however those with low parental monitoring seemed to engage in the more extreme risk taking behaviours or be exposed to inappropriate material.

> *'…I have a lot of friends who [parents did not know about online risks], and they were like, 'we don't know what to do, we don't know how to be safe, we don't know the dangers like…'*
>
> **(IRE2, 2016)**

There was an indication of regret at not having stricter parental supervision that may have protected them from inappropriate material.

'…if I wasn't allowed such freedom with my laptop... But what I say it's on my personal experience that encouraged that freedom, so I don't think I speak like everyone...'

(UK2, 2016)

Positive aspects of the internet

While there was a focus on negative online interactions and the dangers that young people can find themselves in, a number of positive aspects about the online world also emerged. It became quite clear that almost universally, the internet was used as the primary way of communicating with family and social group. This is particularly the case if living in an isolated area or having family and friends living abroad.

'…go beyond your own family and the limited environment in which you live…'

(ITA5, 2015)

The internet was described as somewhere where more introverted individuals could express themselves with more freedom and in turn make more friends than they would in the real world. Online disinhibition would play a part in this phenomenon; while some people found it easier to disclose information about themselves online through computer mediated communication.

'…felt you could message someone who you wouldn't talk to…in real life…'

(IRE1, 2016)

'…it was a way to make friends…if you feel like you are embarrassed or something you can just turn off your computer because you are behind a screen so I thought it was a way to make friends…'

(IRE2, 2016)

The importance of identity and social status on self-esteem

One recommendation youth receive constantly is to keep online personal information private. However, teenagers see their online identity as playing a large role in their social status amongst peers. The more open a young person's social media account is, the more likely it is that they will receive increased friends requests from strangers, therefore increasing social capitol and perceived popularity. In a sense, online popularity can be more important than online safety.

'…they don't [make their profiles private] and they make it public so they can have more 'likes', more contacts. Because that's really what counts the most, right? Because if you don't have many, it means that you're not popular enough and you are conscious of it…'

(ITA4, 2016)

It was also expressed that teenagers invest too much importance on their online image. There is significant time spent trying to build a perfect profile that will attract attention or confirmation through 'likes' and comments while the image that is created may not be in line with their offline personality. Individuals can feel a pressure trying to up to the perceived 'perfect' lives of their peers as portrayed online whereas in reality there is a large discrepancy between peoples offline and online images.

> *'…[friend] posts a lot of pictures online…too much. Boys like to flirt with this girl, but I think...when she puts that pictures people can think she's a different kind of person…'*
>
> **(ITA5, 2016)**

The teenage years can consist of significant insecurity and identity development which the internet can play a large role in constructing. Participants felt part of their identity was recognised online. Having felt different for having certain tastes, identity could be reinforced by locating others with similar interests.

> *'…when I heard there were other people, apart from me, like me, this was very nice…'*
>
> **(ITA3, 2016)**

Advice to young people today

When asked about what advice participants would give to teenagers growing up today based on their own experiences, a number of recommendations were made. Approaching a trusted individual for support when exposed to dangerous or inappropriate content online was widely encouraged. There are reasons to believe that young people would not approach adults for support as they feared over-reactions and the loss of privileges. Teenagers are encouraged to disclose what they are experiencing online as having social support is important in mitigating them against risk.

> *'…I understand why my sister wouldn't talk to my mom because maybe they are not informed enough and they are going to be mad…just talk to people because sometimes older people will realise there is something wrong in a way that you won't…'*
>
> **(IRE2, 2016)**

Summary

In Italy, Ireland and the UK, a large online survey was conducted among 1166 respondents about their online behaviour when they were aged between 12 and 16 years. The respondents, average age 20 years, were asked to look back and report on this period. The sample was unevenly distributed for country and gender. The number of females was more than twice as much that of males. The Irish sample accounted for nearly half of the

respondents. Most respondents possessed Internet devices and used the internet regularly, for example, to listen to music, watch movies, chat and for schoolwork. According to the respondents, parental control was rather limited and parents were not really concerned with making the Internet safer for their kids. Some risky behaviours on the Internet happened more often (e.g. downloading pirated material and sharing photo's/videos) than others (e.g. being harassed/threatened online by text). In general, boys showed more risky behaviour than girls.

Boys were more involved in sexting behaviour than girls, and girls were more often than boys solicited or invited to give sexual information about themselves or to send a sexually suggestive photo or movie of themselves. Older Internet users were more often interested in engaging younger girls to exhibit sexually behaviour. Formal help-seeking behaviour was rare. Only the consultation of a friend occurred for one in three when something bad happened on the Internet. Other formal or informal sources were hardly ever consulted. Offline problem behaviours were asked about, such as excessive alcohol use, playing truant from school, problems with teachers and bad behaviour, and drug use. Relatively few respondents reported these but boys showed more behavioural problems than girls. Therefore boys show more online and offline risk behaviours than girls, and girls are more at risk to be victimized online than boys.

Those most at risk of online sexual solicitation by an adult were:

- Girls, 5 times higher risk than boys
- Those more frequently harassed or threatened (on or offline)
- Those who more often added/accepted unknown people to their friends lists online
- Those who more frequently watched adult pornography as teenagers
- Those who sent someone else a sexual message or request

Four profiles were identified. These are listed by the least to highest risky/vulnerable behaviour and risk for online solicitation.

The **Adapted Adolescent** group was the largest group and had the least number of risk behaviours online or offline, least vulnerability and the least likely to receive sexual solicitations from an adult online.

The **Inquisitive non-sexual** group had lower risk taking offline but higher online risk-taking. They were at low likelihood of receive sexual solicitations, or send sexts.

The **Inquisitive sexual** group demonstrated the highest rate of receiving requests for sexual information. They had a high likelihood of rreceiving sexual solicitations from adults (14 times higher than the adapted adolescents, and 6 times higher than the inquisitive non-

sexual group). It is concerning that this group had the highest likelihood of meeting up in person to engage in a sexual activity.

The **Risk-taking aggressive** category, were the smallest group. They exhibited the highest risk taking on and offline, most likely to both harass and be harassed. They demonstrated real world anti-social behaviour such as problems with authority (parents and teachers), truancy, school exclusion, drug and alcohol use. They had the highest levels of online/offline aggression towards others including peers. However they also had a heightened level of experiencing online/offline victimisation at the hands of others. Thus they were the most likely to receive sexual solicitations from adults – for example 34 times higher than the adapted adolescent, and 15 times higher than the inquisitive non-sexual profile.

Depth interviews conducted with self-referred young people who responded to the surveys demonstrated that there were a range of behaviours that many young people engage in online which, at the time of engagement, did not register as particularly dangerous, risky or negative. However, many youth did recognize that they are aware of these dangers, but rarely sought support or help in dealing with them.

6.0 Implications for policy and practice

6.1 Making collaborative practice work- models of good practice

There are a number of key implications for best practice in policing online CSA deriving from the ISEC study. These concern different levels of policing work, including but not limited to international management of online CSA, collaboration with industries, training and preparation of police officers, development of knowledge and skills for specialists in online CSA, investigation of cybercrime and its prosecution.

1. **Clear shared international definitions of online CSA – supported by an updated UNCRC which includes cyber abuse**
   It is clear from the ISEC evidence that despite some good examples of agency collaboration involved in policing online CSA, policing would benefit from a more consistent and structured definition of online CSA across countries, which should start with a shared legal definition of child (age of informed consent to sexual relations) . The lack of a shared international definition is one of the biggest obstacles in investigating and prosecuting online child sexual abuse cases. This would allow for better collaboration and development of shared knowledge between police forces and more effective collaboration between police forces and industry, within and across countries.

2. **Policy, legislation and practice must become more responsive and able to rapidly adapt to an evolving cyberspace** as industries are necessarily doing, and police forces need to always be up-to-date with best practice in the investigation and prevention of emerging cybercrime.

3. **The development of systematic policing and industry collaboration.** Nationally co-ordinated law enforcement and industry collaboration, in some instances this collaboration could be at international level. The industry case studies highlighted some examples of good practice and it is clear that there is currently some collaboration but this is at best sporadic and the level of collaboration varies by country and at national level by police force. There is a willingness on the part of law enforcement to engage in a more systematic and co-ordinated way. Some industry would welcome more collaboration but others are concerned about potential reputational damage and differences in organisational goals and approach. It is clear that there is much to be gained from a more joined up working approach in terms of ensuring that policing knowledge is up to date and ultimately in securing a safer Internet for children, this approach would also ensure that industry is more knowledgeable about policing practice and online offending behaviour. Industry should contribute as follows:

1. Industry mentoring of specialist police officers
2. Named industry points of contact for police forces
3. Joint industry and law enforcement task forces – which could include other agencies
4. Industry contribution to law enforcement training

The problem is that this activity requires central co-ordination and monitoring at national and EU level the Europol Cybercrime Centre (EC3) Academic Advisory Board could take a lead in helping to develop some good practice guidance for example and at national level organisations like the UK Council for Child Internet Safety could help to facilitate the work.

6.2 Training recommendations

In this context, the ISEC project findings suggest that training and collaboration with industries are critical issues to take into account in the effective prevention, investigation and prosecution of online CSA.

1. **The development of specialist training at a basic level for all rank and file officers, the enhancement of more advanced training for specialist officers**
   While the first issue necessarily concerns the officers' preparedness to practically deal with the cases including: Knowledge about online CSA crimes, child and offender behaviour online; an understanding of the relevant legislation: the practice of collecting evidence; the effective and supportive interviewing of child victims of online abuse; the interviewing of child offenders. The second issue concerns the best practice for monitoring the web in preventing such cases, as well as having fast, timely contacts with the potential victims (e.g., through online reporting), to rapidly tracking the origin of a potential cybercrime, and in using industry knowledge to develop more sensitive approaches to the identification of potential offenders through new algorithms, and more sophisticated and comprehensive strategies of prevention for online crimes.

6.3 Effective policing of online CSA cases

The ISEC study allowed us to develop some key points regarding best practice of policing CSA. Each of the points below should be considered as essential in effectively policing online CSA cases:

1. **Knowledge of Relevant National Legislation.** Development of knowledge about national laws on online CSA among general police officers. While knowledge about national laws on child sexual abuse is widely known among general POs, some of them may be not updated on more recent law development in the field of online

CSA. As many reports of potential grooming cases are made in person to a general police constable, it is critical that he or she is fully aware of the law and the potential crime committed to allow for early identification and understanding of online cases.

2. **Knowledge of Relevant International Legislation**. Development of knowledge about international laws on online CSA and guidelines to treat online CSA cases among experts. As technologies expand, and cybercrimes also expand, it is critical that experts are aware of international laws and guidelines to combat online CSA. This will give them more information and tools to prevent online CSA crimes, also fostering further effective collaborations with international police forces, EC3, and industries is of great importance.

3. **Increased collaboration with third sector partners and non-profit organizations**. Third sector partners and non-profit organizations have proved very effective in providing police forces with instruments and tools that can help in monitoring the Internet and managing risks of child abuse (such as online and offline hotlines for reporting online grooming cases, software algorithms to detect indecent images of children, etc.). These collaboration should be further strengthened.

4. **Collection of evidence from ICT devices in Potential Online CSA cases-** Law enforcement should always collect evidence related to Information and Communication Technology (ICT) devices in potential cases of online CSA. This is already done by most police officers, but it is worth remembering the importance of collecting evidence following the appropriate protocols, in order to help with investigations and eventually with the prosecution of the offenders.

5. **Always investigate online activities of child sexual offenders**. There is no reason to believe that in the era of ICT, child sexual offenders only offend offline, and this could allow investigators to detect further crimes against minors that could be not immediately observed.

6. **Always investigate the offline activities of online groomers and those who collect indecent images of children.** -This is usual practice, but it is worth remembering that while some offenders will not immediately have a face-to-face meeting with the child in order to sexually abuse him or her, many may have a network of relationships with people who are directly involved with online and offline CSA or could even be part of a ring of abusers.

7. **Use the network of collaborations**. It is common practice that officers who are highly trained and may be well called experts deal with online CSA cases. However, cases of online CSA often require that different professionals should cooperate in effectively responding to such cases. For example, especially when dealing with difficult cases, a password decryption could require an expert programmer, a fast

detection and prevention of ongoing crimes could require a tight collaboration with industries, an undercover investigation could require psychological support, a collection of evidence in offline contexts could require a legal expert. It is therefore important to ensure that a network of professionals with relevant expertise are involved.

6.4 Improving collaboration with other professionals

Many professionals are often in the process of preventing online CSA and dealing with actual cases. Of course, school is a place where children have to learn about the risks of the Internet, and it is evident that attention to school education has been given as a priority for preventing online CSA cases. However, it is important to continue collaborating with schools, but at the same time to improve the collaboration with other professionals who can be of great help when online grooming or even online CSA has already happened. In this context, social workers and psychologists may be helpful in both supporting the child and helping with interviews. This would mean protecting the child (and the entire family in some cases) from very negative psychological consequences, such as depression or posttraumatic stress disorder. The identification of groups of youth who appear most at risk of CSA through an online approach need to be further explored in terms of training opportunities for police officers and other professionals. This will aid identification for those most at risk for preventative action, but also help to tailor interventions. Thus the risk-taking aggressive youth indicate highest risk for such solicitation, but are also perpetrators of other harmful behaviour towards their peers online. This is likely to involve complex intervention. In contrast the Inquisitive sexual have similarly high risk of solicitation online but can be identified more as victims of aggressive behaviour of others. These profiles need testing in further research, but can serve to identify more tailored training to different types of online behaviour and risk. It is unlikely that these two groups will change their behaviour due to generic online safety training. They have a likelihood of suffering mental health problems and disadvantage, and these need to be further identified in order to identify multi-agency support and reduce the prevalence and impact of harmful CSA initiated online.

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.

Arnett, J. J. (1995). Adolescents' uses of media for self-socialization. *Journal of Youth and Adolescence*, *24*(5), 519-533.

Babchishin, K. M., Hanson, R. K., & Hermann, C. A. (2011). The characteristics of online sex offenders: A meta-analysis. *Sexual abuse: a journal of research and treatment*, *23*(1), 92-123.

Baker, K. (2012). Contagious Diseases Acts and the Prostitute: How Disease and the Law Controlled the Female Body. *The UCLJLJ*, *1*, 88.

Ball, R. and Lilley, C. (2014). *The experiences of children aged 11-12 on social networking sites.* London, UK: NSPCC.

Baumgartner, S. E., Valkenburg, P. M., & Peter, J. (2010). Unwanted online sexual solicitation and risky sexual online behaviour across the lifespan. *Journal of Applied Developmental Psychology, 31,* 439-447.

Carr, J. (2010). *The internet dimension of sexual violence against children.* In Council of Europe's 'Protecting Children from Sexual Violence: A comprehensive Approach' working paper series.

Carr, J. (2014). Observations on the implementation of Article 23 of the Lanzarote Convention concerning the online solicitation of children for sexual purposes, otherwise known as 'grooming'. *Document prepared in cooperation with the Secretariat of the Lanzarote Committee as part of the Committee of the Parties to the Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse (T-ES).*

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

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

Davidson, J., & Gottschalk, P. (Eds.). (2010). *Internet child abuse: Current research and policy*. New York, NY: Routledge.

Davidson, J., Grove-Hills, J., Bifulco, A., Gottschalk, P., Caretti, V., Pham, T., & Webster, S. (2011). Online abuse: Literature review and policy context. European Online Grooming Project. Available from: www.europeanonlinegroomingproject.com/media/2080/eogp-literature-review.pdf

Davidson, J., & Martellozzo, E. (2008). Protecting vulnerable young people in cyberspace from sexual abuse: Raising awareness and responding globally, *Police Practice and Research: An International Journal, 9*(4), 277-289.

Davidson, J., & Martellozzo, E. (2012). Exploring young people's use of social networking sites and digital media in the internet safety context: A comparison of the UK and Bahrain. *Information, Communication and Society,* 1-21.

DeMarco, J., & Davidson, J. (2015). ISEC: Illegal use of the internet – Police and industry collaboration: Annual Report – Progress report.

DeMarco, J. N., Davidson, J. C., Scally, M. & Long, E. (2015). ISEC Illegal Use of the Internet: Policing, collaboration and victimisation—A Review of the Literature. *Document prepared for the European Commission initiative in dealing with cybercrime and cybersecurity.*

Education, Audiovisual and Culture Executive Agency (2009). *Summary report, Education on online safety in schools in Europe*. Brussels, BE: EURYDICE.

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: An international, interdisciplinary forum for research, theory and practice, 16*(2), 223-235. DOI:10.1080/13552601003760014

EU Kids Online. (2014). *EU Kids Online: findings, methods, recommendations*. London, UK. Retrieved from http://eprints.lse.ac.uk/60512/

European Parliament of Justice, Freedom and Security, Policy department citizen's rights and constitutional affairs. (2015). Combatting child sexual abuse. Retrieved from http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536481/IPOL_STU(2015)536481_EN.pdf

Finkelhor, D., Mitchell, K. J., & Wolak, J. (2000). *Online Victimization: A Report on the Nation's Youth*. US Department of Justice, Office of Justice Programs, Office of Juvenile Justice and Delinquency Prevention.

Gallagher, B., Fraser, C., Christmann, K., & Hodgson, B. (2006). *International and Internet child sexual abuse and exploitation*. Huddersfield, UK: University of Huddersfield.

Harvard Health (2008) *Protecting Children and Teens from cyber-harm,* Harvard Medical Health Letter, Harvard Medicine.

Heslip, J. C. (2013). *The Brave New Online World of Teens and a Call to Action for Educators*. A Research Paper Presented to the Gordon Albright School of Education In Partial Fulfillment of the Requirements For the Degree of Master of Education.

Houtepen, J. A., Sijtsema, J. J., & Bogaerts, S. (2014). From child pornography offending to child sexual abuse: A review of child pornography offender characteristics and risks for cross-over. *Aggression and Violent Behavior*, *19*(5), 466-473.

International Centre for Missing and Exploited Children (2006). *Child pornography: model legislation and global review*. Retrieved, May 2, 2007 from icmec.org/en_X1/pdf/English_2nd_Edition.pdf

ITU (2016). *ICT facts and figures 2016*. Geneva, Switzerland, ITU.

Johnson, G. M. (2010). Internet Use and Child Development: The Techno-Microsystem. *Australian Journal of Educational & Developmental Psychology*,*10*, 32-43.

Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). Risks and safety on the internet. *The perspective of European children. Final findings from the EU Kids Online survey*, 9-16.

Livingstone, S., & Smith, P. K. (2014). Annual Research Review: Harms experienced by child users of online and mobile technologies: the nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of child psychology and psychiatry*, *55*(6), 635-654.

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 cyber crime. *International Journal of Police Science & Management*, *12*(4), 516-525.

Mascheroni, G., & Cuman, A. (2014). *Net Children Go Mobile: Final Report. Deliverables D6.4 & D5.2*. Milano.

McGrath, M. G., & Casey, E. (2002). Forensic Psychiatry and the Internet: Practical Perspectives on Sexual Predators and Obsessional Harassers in Cyberspace. *J Am Acad Psychiatry Law, 30*, 81–94.

Ministry of Justice. (2015). Revenge Porn: The Facts. Available from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/405286/revenge-porn-factsheet.pdf

Mitchell, K. J., Jones, L. M., Finkelhor, D., & Wolak, J. (2013). Understanding the decline in unwanted online sexual solicitations for U.S. youth 2000-2010: findings from three Youth Internet Safety Surveys. *Child Abuse & Neglect*, *37*(12), 1225–36. doi.org/10.1016/j.chiabu.2013.07.002

NCMEC. (2015). Child sexual exploitation. Available from www.missingkids.com/Exploitation

Nguyen, M., Bin, Y. S., & Campbell, A. (2012). Comparing online and offline self-disclosure: A systematic review. *Cyberpsychology, Behavior, and Social Networking*, *15*(2), 103-111.

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

Ofcom. (2014). *Children and Parents: Media use and Attitudes Report.* London, UK: Ofcom.

Prendergast, W. E. (1991). *Treating sex offenders in correctional institutions and outpatient clinics: a guide to clinical practice*. Binghamton, NY: Haworth Press.

Prensky, M. (2001). Digital natives, digital immigrants part 1. *On the horizon*, *9*(5), 1-6.

Priebe, G., Mitchell, K. J., & Finkelhor, D. (2013). To tell or not to tell? Youth's responses to unwanted Internet experiences. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 7*, article 6. doi: 10.5817/CP2013-1-6.

Quayle, E. (2010). Child Pornography. *Handbook of Internet Crime*, 343-368.

Quayle, E., Jonsson, L., & Lööf, L. (2012). Online behaviour related to child sexual abuse. *Interviews with affected young people. ROBERT, Risktaking online behaviour, empowerment through research and training. European Union & Council of the Baltic Sea States*.

Shearing, C. D., & Stenning, P. C. (1981). Modern private security: its growth and implications. *Crime and justice*, 193-245.

Shearing, C. D., & Johnston, L. (2013). *Governing security: Explorations of policing and justice*. Routledge.

Staksrud, E., & Livingstone, S. (2009). Children and online risk. *Information, Communication & Society*, *12*(3), 364–387.

Suler, J. (2004). The online disinhibition effect. *Cyberpsychology & behavior*,*7*(3), 321-326.

Tidwell, L. C., & Walther, J. B. (2002). Computer-mediated communication effects on disclosure, impressions, and interpersonal evaluations: Getting to know one another a bit at a time. *Human communication research*, *28*(3), 317-348.

Wachs, S., Wolf, K. D., & Pan, C. C. (2012). Cybergrooming: Risk factors, coping strategies and associations with cyberbullying. *Psicothema*, *24*(4), 628-633.

Walsh, C. (2011). Youth justice and neuroscience: A dual-use dilemma. *British Journal of Criminology*, *51*(1), 21-39.

Walther, J. B. (1996). Computer-mediated communication impersonal, interpersonal, and hyperpersonal interaction. *Communication research*, *23*(1), 3-43.

Webster, S., Davidson, J., Bifulco, A., Gottschalk, P., Caretti, V., Pham, T., Grove-Hills, J., Turley, C., Tompkins, C., Ciulla, S., Milazzo, V., Schimmenti, A., & Craparo, G. (2012). *Final report: European Online Grooming Project*. London, UK: European Commission Safer Internet Plus Programme.

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*, *8*(3), 269-282.

Wells, M., & Mitchell, K. J. (2014). Patterns of internet use and risk of online victimisation for youth with and without disabilities. *Journal of Special Education, 48*(3), 2014-213.

Whittle, H. C., Hamilton-Giachritsis, C. E., & Beech, A. R. (2014). “Under His Spell”: Victims’ Perspectives of Being Groomed Online. *Social Sciences*, *3*(3), 404-426.

White, J. L., Moffitt, T. E., Caspi, A., Bartusch, D. J., Needles, D. J. and Stouthamer-Loeber, M. (1994). Measuring impulsivity and examining its relationship to delinquency. *Journal of Abnormal Psychology*, *103*(2), 192.

Williams, K. S. (2003). Controlling Internet child Pornography and Protecting the Child. *Information & Communication and Technology Law*, *12*(1), 245-261.

Williams, K. S. (2004). Child pornography law: Does it protect children? *Journal of Social Welfare and Family Law, 26*(3), 245-261.

Wolak, J., & Finkelhor, D. (2013). Are crimes by online predators different from crimes by sex offenders who know youth in-person? *Journal of Adolescent Health. 53*. 736-741.

Wolak, J., & Finkelhor, D. (2011). *Sexting: A typology. Crimes Against Children Research Center*. Durham, NH.

Wolak, J., Finkelhor, D., & Mitchell, K. (2008). Is talking online to unknown people always risky? Distinguishing online interaction styles in a national sample of youth Internet users. *CyberPsychology & Behavior*, *11*(3), 340-343.

Wolak, J., Finkelhor, D., Mitchell, K. J., & Ybarra, M. L. (2008). Online ‘‘predators’’ and their victims: Myths, realities, and implications for prevention treatment. *Am Psychol., 63*, 111–28.

Wolak, J., Mitchell, K. J., & Finkelhor, D. (2003). Escaping or connecting? Characteristics of youth who form close online relationships. *J Adolesc,. 26*, 105–19.

Wolak, J., Mitchell, K., & Finkelhor, D. (2007). Unwanted and Wanted Exposure to Online Pornography in a National Sample of Youth Internet Users. *Pediatrics. 119* (2), 247-257.

Appendices

Appendix I: Information for participants in Work Package 1

EU Online Child Safety Project
Stakeholder Information

Thank you for agreeing to participate in this study investigating the cooperation between law enforcement and industry whilst working together to promote safer online experiences for children and adolescents.

The interview should last approximately one hour and will be audio-recorded and stored for future thematic analysis.

The discussion will focus on your understanding of current issues surrounding online Childhood Sexual Abuse (CSA) within a political and criminal justice perspective. Specifically, we hope to explore in greater detail precisely what agencies/authorities/organizations such as you think about current practices on a front line level, but also within a legal and political framework. We are also interested in identifying key industry partnerships in the prevention and intervention of online CSA.

Should you have any questions please feel free to ask the researcher before the session; they will be happy to provide you with any additional information you may require. The researchers contact details can be found below. All responses gathered will be treated with the greatest level of confidentiality in line with both British Society of Criminology and British Psychological Society Codes of Conduct and Ethics. The information itself will be stored in line with data protection guidelines. Any indications of your true identity will be replaced with pseudonyms and should you wish to withdraw from the study at any point, please inform the researcher.

If you agree to participate, please indicate your consent with the form provided.

Thank you for your participation.

Kindest Regards,

Jeffrey DeMarco
Project Research Fellow (ISEC)
Research Fellow for the Centre of Abuse and Trauma Studies (CATS)

Williams Building G02,
Middlesex University
The Burroughs, Hendon

London, NW4 4BT

www.cats-rp.org.uk/
j.demarco@mdx.ac.uk

Participant ID #:

EU Online Child Safety—Stakeholder Interviews

Name of Researcher:

1. I confirm that I have been explained my participation in the current study, and understand the information sheet provided. I have had the opportunity to ask questions for any items that were unclear.

2. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving reason. I am able to do this by providing the above participant ID code to the researcher, who in turn will remove my information from the data set.

3. I agree that the information I give during the study can be used in any related publications, such as reports and academic articles.

4. I understand that my interview will be audio-recorded and subsequently transcribed verbatim for further analysis. In accordance with the guidelines of the British Criminological Association and the British Psychological Society, both my anonymity and confidentiality will be ensured. Where necessary, pseudonyms will be used to protect my identity.

5. I agree that anonymised quotes can be used in any publications related to the study.

6. I agree to take part in the above study.

_____	_____	_____
Name of participant	Date	Signature

_____	_____	_____
Researcher	Date	Signature

EU Child Online Safety Project
Law enforcement and industry practices

Thank you again for participating in the current study.

The research has been developed in response to increased concern regarding the need to identify those children and young people most likely to be victimised by peers and/or adults online and to further equip both law enforcement and industry with the technological tools to enable effective preventative strategies and measures. Whilst great progress has been made in educating children about internet safety, policing and industry practices in preventing online abuse remain under researched. The collaboration between these two aforementioned projects also needs clarification.

It is therefore essential to draw together elements of good practice to develop models that can be standardised at an EU and global level It is for this reason that you had been selected to participate in today's interview. The research needed to draw upon real time ground level research with stakeholders in various positions surrounding the field of online child safety.

If you would like further details about our work on the current research initiative, please visit the project site at www.euchildsafetyonlineproject.com and remember to check in regularly for project updates. Additionally, you may be interested in some of our previous work related to online abuse, child exploitation and grooming behavior (www.europeanonlinegroomingproject.com) and the ROBERT online risk-taking behavior project (www.childcentre.info/robert). Further details of the team at Middlesex and associated research projects can be found on the Centre for Abuse and Trauma Studies website (cats-rp.org.uk/index.htm).

Finally, should you have any further questions or queries related to this phase of the project or additional phases, please do not hesitate to contact either our Principal Investigator Professor Julia Davidson (j.davidson@mdx.ac.uk) or the Project Research Fellow, Mr. Jeffrey DeMarco (j.demarco@mdx.ac.uk).

Thanking you once again for your assistance and time for such an important area of research. Your involvement is greatly appreciated.

Kindest Regards,

Jeffrey DeMarco
Project Research Fellow (ISEC)
Research Fellow for the Centre of Abuse and Trauma Studies (CATS)

Williams Building G02, Middlesex University, The Burroughs, Hendon, London, NW4 4BT
www.cats-rp.org.uk/
j.demarco@mdx.ac.uk

Appendix II: Work Package 1 Interview Schedule

EU Online Child Safety: Stakeholder Interview Schedule

1) Contemporary Practice

Childhood Sexual Abuse (CSA) is a serious problem faced by contemporary society that transgresses international boundaries. The perpetration of CSA through Information and Communication Technologies (ICT's) such as the internet can make the prevention and intervention of such crimes exponentially more difficult to achieve.

a. Consider how your agency/police authority/organisation deals with the reporting of online CSA.
   - ↗ Examples of good practice
   - ↗ Examples of poor practice
   - ↗ Recommendations for improving services provided

b. Within your police force/authority/organisation, please describe the different partnerships working together in responding to allegations of online CSA.
   - ↗ Local and national
   - ↗ Across different police authorities
   - ↗ With local and national government
   - ↗ Community partnerships (i.e. local businesses, charities)

c. Given the global nature of the problem, and the ability for perpetrators to reach potential victims across geographical and emotional boundaries, discuss the importance of international collaborations.
   - ↗ Interpol
   - ↗ Europol
   - ↗ WHO
   - ↗ United Nations

2) Governmental policy and legislation

Although CSA can be a tangible act occurring in the physical world, the use of ICT's such as e-mail, webcams and mobile phones often makes the criminalisation and policing of online CSA both difficult and geo-politically complex.

d. Discuss your understanding of existing policy designed to assist in the prevention of online CSA.

- ↗ Data sharing and data protection
- ↗ Online material
- ↗ Direct CSA

e. What are some of the legal difficulties in dealing with online perpetrators of CSA?
   - ↗ Invisibility
   - ↗ Anonymity
   - ↗ Jurisdiction
   - ↗ Physical evidence
   - ↗ Resources (i.e. technological? Financial?)

f. Please provide some examples of the distinctiveness that your police force/authority/government applies to online CSA in comparison to direct CSA.
   - ↗ Detection
   - ↗ Prosecution and conviction
   - ↗ Penalties and sentencing
   - ↗ Post-sentence

3) Importance of industry practice

The use of the internet and other ICT's has exploded over the last decade. As a result, much of our daily routine is spent online. This includes activities such as shopping via websites and socialising through social media platforms. Households using Google, Twitter and Facebook have proliferated

g. Which ICT organisations has your police force/authority worked in collaboration with when dealing with online crime (with particular reference to online CSA)? If none, what organisations moving forward do you feel should work in partnership with the police and why?
   - ↗ Detection
   - ↗ Prosecution and conviction
   - ↗ Penalties and sentencing
   - ↗ Post-sentence

h. Please provide any details of collaborative agreements with industry partners that your police force/authority has. All details will be an

i. How important are these partnerships for your force/authority in tackling online CSA? If you do not work with any industry partners, what impact do you think these partnerships could have?

Appendix III: Work Package 1 Survey

EU Online Child Safety Project
Survey Participant Information

Thank you for agreeing to participate in this study investigating practice in law enforcement and industry whilst working together to promote safer online experiences for children and adolescents.

The survey should take you no longer than ten to fifteen minutes to complete.

The questions will be directed towards your experience within policing and revolve around current police and industry practice on dealing with online crimes against children and adolescents.

Specifically, we hope to explore in greater detail precisely how online crimes related to children, such as grooming and indecent images, are dealt with throughout the criminal justice process, from the point of discovery through to sentencing, conviction and resulting sentence. We are also interested in identifying key partnerships in the prevention and intervention of online CSA from a policing perspective.

Should you have any questions please feel free to contact Jeffrey DeMarco (j.demarco@mdx.ac.uk) the project Research Fellow; he will be happy to provide you with any additional information you may require. All responses gathered will be treated with the greatest level of confidentiality in line with both British Society of Criminology and British Psychological Society Codes of Conduct and Ethics. The information itself will be stored in line with UK data protection guidelines. At no point will you need to indicate your true identity, and if you wish to withdraw following participation, you may do so by providing the research team with the ID number you will receive post-completion.

If you agree to participate, please indicate your consent by ticking the appropriate box below.

Thank you for your participation.

The ISEC Research Team

- ☐ I agree to take part in the above study
- ☐ I do not agree to take part in the above study

Section 1: Demographics and roles

1. Gender □ Male □ Female
2. Age: _____
3. Rank: _____
4. Current role/Department: _____
5. Police force: _____
6. Length of overall service (years): _____
7. Length of service in current role (months): _____
8. Have you ever dealt with any form of cybercrime before? □ Yes □ No
9. If 'Yes' to above, how often? □ Yearly □ Monthly □ Weekly □ Daily

---

Section 2: Experience and training

1. Over the last ten years, have you been involved in the investigation of online child abuse involving (please tick all that apply):

   □ Image collection
   □ Image production
   □ Image distribution
   □ Online grooming
   □ Sexting
   □ Other (please specify in the space provided)

2. In the last ten years, have any of your cases involved the following behaviours (please tick all that apply):

- ☐ Trolling
- ☐ Flaming
- ☐ Harassment
- ☐ Cyber-bullying
- ☐ Impersonation/identity theft
- ☐ Online sexual abuse
- ☐ Other (please specify in the space provided)

3. Approximately how many Computer Mediated Crimes Against Children (CMCAC) have you worked on in the past 10 years: _____

4. Have you received any training in the area of CMCAC (Please tick all that apply):

   - ☐ General
   - ☐ Specialised
   - ☐ No training in this area

5. If you responded to either general or specialised training above, please briefly describe what this included and who provided the training in the space provided:

6. Have you ever received training in interviewing child victims of sexual abuse?

   - ☐ Yes
   - ☐ No

7. If you responded with yes in question 6, did it include CMCAC?

   - ☐ Yes
   - ☐ No

Section 3: The Criminal Justice Process

1. How are computer mediated crimes against children (CMCAC) typically reported in the first instance?
    - ☐ In person to a Police Constable or constabulary
    - ☐ Telephone to the local police authority
    - ☐ Telephone to a special high tech crime unit
    - ☐ The same manner as non-CMCAC, there is no difference
    - ☐ Other (please specify): _____

2. Are child protection teams always involved?

    - ☐ Yes
    - ☐ No
    - ☐ Not available

3. Are any other professionals involved with the investigation outside of policing?

    - ☐ Social Workers
    - ☐ Psychologists
    - ☐ Victim Support representatives
    - ☐ Counsellors
    - ☐ Family Support Workers
    - ☐ Other (please specify): _____

4. Are CMCACs always referred to specialist units within the police?

    - ☐ Yes
    - ☐ No

5. Does your area/authority have a Multi-agency Safeguarding Hub (MASH)?

    - ☐ Yes
    - ☐ No

6. If yes, what proportion of cases are referred to the MASH?

    - ☐ None
    - ☐ Less than 10%
    - ☐ One third
    - ☐ One half
    - ☐ More than 75%

- All cases
- Don't know

7. Please describe the reasons behind your response to the previous question and who/where they are referred if applicable.

8. To the best of your knowledge, what proportion of the CMCAC cases are referred to your force by CE-OP?

   - None
   - Less than 10%
   - One third
   - One half
   - More than 75%
   - All cases
   - Don't know

9. In your current role, do you interview child sex offenders (SO's)?

   - Yes
   - No

10. If you responded yes to the above question, do you always ask questions related to possible internet related activities?

    - Always
    - Sometimes if it seems relevant
    - Not usually
    - Never
    - This question is not applicable to me

11. What evidence is typically collected in an investigation involving child sexual abuse(please select all that are applicable):

    - Mobile phones
    - Tablets
    - Gaming consoles

- Laptops
- Hard drives
- DNA evidence (blood, hair)
- Fingerprints
- Witness statements
- Character statements
- Cyber-related (dialogue online; IP addresses)
- Other

12. To the best of your knowledge, what proportion of CMCAC cases are discontinued by the Crown Prosecution Service? (Please leave blank if you are unsure)

    - Less than 10%
    - 25%
    - 50%
    - More than 75%

13. In your current role, do you conduct specialised interviews with victims of Childhood Sexual Abuse?

    - Yes
    - No

14. If you responded yes to the above question, do you routinely explore the possibility that the victims were abused via the internet or using Information and Communication Technologies?

    - Yes
    - No
    - Sometimes when it seems relevant

15. How would you describe the current training surrounding the policing and investigation of Online Childhood Sexual Abuse?

    - Excellent
    - Adequate
    - Inadequate

16. Please indicate how prepared you feel as a consequene of your training on the scale below.

Extremely unprepared ----------Extremely Prepared

1 2 3 4 5

17. If unprepared, what elements/changes would be useful?
18. If prepared, please comment on the positive elements:

19. Are Informatin and Communication Technologies devices (i.e. laptop, mobile phone, tablets, etc.) routinely analysed throughout sentences served in the community?

- ☐ Yes
- ☐ No
- ☐ Do not know

Section 4: Collaborative practice

1. Please indicate any partnerships or collaborative organisations/areas your force or department has worked with in policing Computer Mediated Crimes Against Children (CMCAC):

- ☐ Education (schools)
- ☐ Community groups (charities dealing with young people)
- ☐ Industry partners (Facebook, Twitter, smaller online firms)
- ☐ Victim support centres
- ☐ Resettlement/Proabation services
- ☐ Other: _____
- ☐ None

2. If you responded yes to the above, could you please briefly describe the work you have done with the various partners:

3. In your own opinion, how might law enforcement agencies better collaborate with industry partners (Please tick all that apply):

    - ☐ Data sharing
    - ☐ Communication
    - ☐ Joint task forces
    - ☐ Secondments
    - ☐ Seminars/Professional Development Courses
    - ☐ Other: _____

Section 5: Legislation

1. Which of the following legislation in the area of Computer Mediated Crimes Against Children (CMCAC) are you familiar with? Please tick all that apply.

    - ☐ Sexual Offences Act 2003
    - ☐ Police and Justice Act 2006
    - ☐ Criminal Justice and Immigration Act 2008
    - ☐ European Union Directive 2013
    - ☐ Other: _____

2. Thank you for completing the survey. Is there anything else you would like to add:

Appendix IV: Information for participants in Work Package 2

EU Online Child Safety Project
Survey Participant Information

Thank you for agreeing to participate in this study investigating your experience of online behaviour in your adolescent years. The purpose of this study is to describe the behaviours of young adults aged between 18 and 25 years old when engaging in online activities as teenagers, as well as to explore both the positive and negative experiences they had online during this time of their lives. If you are currently feeling mentally or emotionally vulnerable, we would suggest you do not complete the survey if you think that these questions will distress you.

This project is funded by the European Commission, Directorate C-Schengen, Unit C4-Internal Security Fund (Home/2013/ISEX/AG/INT/4000005230). The project as a whole is co-ordinated by Professor Julia Davidson of the Centre for Abuse and Trauma Studies at Middlesex University (United Kingdom), with partners at Tilburg University (Netherlands), FDE Institute of Criminology and Kore University of Enna (Italy). Sample participants will be recruited from Ireland, Italy and the United Kingdom.

Should you have any questions please feel free to contact Jeffrey DeMarco (j.demarco@mdx.ac.uk) the project Research Fellow; he will be happy to provide you with any additional information you may require. All responses gathered will be treated with the greatest level of confidentiality in line with both British Society of Criminology and British Psychological Society Codes of Conduct and Ethics. The information itself will be stored in line with UK data protection guidelines. At no point will you need to indicate your true identity, and if you wish to withdraw following participation, you may cease responding at any time however, please note that once you have completed the survey, because it is anonymous, it will not be possible for your data to be removed or deleted, as the researchers have no method of identifying your input from any others.

Should any of the issues discussed above, or subsequently with your participation on the survey lead to you feeling especially concerned about the effect participating in this study has had on you, the following services may be useful to you.

	Phone	**Email**	**Website**
Samaritans (24-hour helpline)	08457 90 90 90	jo@samaritans.org	www.samaritans.org
Mind (24 hour helpline—other	0300 123 3393	info@mind.org.uk	www.mind.org.uk

in-services range from 08h30 to 18h00, Monday to Friday)			
PAPYRUS (Helpline 10h00-22h00 Monday to Friday; 14h00 to 17h00 weekends and Bank holidays)	0800 068 41 41	pat@papyrus-uk.org	www.papyrus-uk.org
Rape Crisis England & Wales **(Line open from 12h00-14h30 and 19h00-21h30 daily)**	0808 802 9999	rcewinfo@rapecrisis.org.uk	ww.rapecrisis.org.uk
The Survivors Trust **(Helpline in development)**	01788 550554	info@thesurvivorstrust.org	www.thesurvivorstrust.org
Victim Support (Weekdays 08h00-20h00; Weekends 09h00-19h00; Bank Holidays 09h00-17h00)	08 08 16 89 111	supportline@victimsupport.org.uk	www.victimsupport.org.uk

Please take the time to read each question carefully. Your participation is greatly appreciated and will assist us in understanding the online behaviours and positive and negative experiences of young people when they go online. The survey should take approximately 15 minutes. Please ensure you understand this Information Sheet before you agree to begin the survey and direct any further queries to Jeffrey DeMarco as indicated above.

If you agree to participate, please indicate your consent by ticking the appropriate box on the next page.

Thank you for your participation.

The ISEC Research Team

THIS WILL BE PLACED ONLINE—PARTICIPANTS WILL BE ASKED TO SELECT WHETHER THEY AGREE OR DISAGREE.

EU Online Child Safety—Victim Experience Survey

Name of Researcher:

1. I confirm that I have read the information sheet provided and understand my involvement in the current study. I have been adequately and accordingly explained the details surrounding the research I am about to participate in.

2. I have taken the opportunity to elaborate upon any questions I may have had.

3. I have been properly provided with answers to those questions.

4. I understand that my participation is voluntary and that I am free to withdraw at any time

5. I agree that the information I give during the study can be used in any related publications, such as reports and academic articles

6. It has been made clear that this study is being conducted in accordance with the guidelines of the British Criminological Association and the British Psychological Society, both my anonymity and confidentiality will be ensured

    - o I AGREE WITH THE ABOVE
    - o I DISAGREE WITH THE ABOVE

EU Child Online Safety Project
Victim Experience Online

Thank you again for participating in the current study.

The research is funded by the European Commission ISEC fund and has been developed in response to increased concern regarding the need to identify those children and young people most likely to be victimised by peers and/or adults online and to further equip both law enforcement and industry with the technological tools to enable effective preventative strategies and measures. Whilst great progress has been made in educating children about internet safety, further knowledge is needed in understanding various factors that lead to vulnerabilities, resilience and differing adult outcomes.

If you feel especially concerned about the effect participating in this study has had on you, the following services may be useful to you.

	Phone	**Email**	**Website**
Samaritans (24-hour helpline)	08457 90 90 90	jo@samaritans.org	www.samaritans.org
Mind (24 hour helpline— other in-services range from 08h30 to 18h00, Monday to Friday)	0300 123 3393	info@mind.org.uk	www.mind.org.uk
PAPYRUS (Helpline 10h00-22h00 Monday to Friday; 14h00 to 17h00 weekends and Bank holidays)	0800 068 41 41	pat@papyrus-uk.org	www.papyrus-uk.org
Rape Crisis England & Wales (Line open from 12h00-14h30 and 19h00-21h30 daily)	0808 802 9999	rcewinfo@rapecrisis.org.uk	ww.rapecrisis.org.uk
The Survivors Trust (Helpline in development)	01788 550554	info@thesurvivorstrust.org	www.thesurvivorstrust.org
Victim Support (Weekdays 08h00-20h00; Weekends 09h00-19h00; Bank Holidays 09h00-17h00)	08 08 16 89 111	supportline@victimsupport.org.uk	www.victimsupport.org.uk

If you would like further details about our work on the current research initiative, please visit the project site www.euchildsafetyonlineproject.com and remember to check in regularly for project updates. Additionally, you may be interested in some of our previous work related to online abuse, child exploitation and grooming behavior (www.europeanonlinegroomingproject.com) and the ROBERT online risk-taking behavior project (www.childcentre.info/robert). Further details of the team at Middlesex and associated research projects can be found on the Centre for Abuse and Trauma Studies website (www.cats-rp.org.uk).

Finally, should you have any further questions or queries related to this phase of the project or additional phases, please do not hesitate to contact either our Principal Investigator Professor Julia Davidson (j.davidson@mdx.ac.uk) or the Project Research Fellow, Mr. Jeffrey DeMarco (j.demarco@mdx.ac.uk).

Thanking you once again for your assistance and time for such an important area of research. Your involvement is greatly appreciated.

Kindest Regards,

Professor Julia Davidson and Jeffrey DeMarco

EU Online Child Safety Project
Depth Interviews Participant Information

Thank you for agreeing to participate in this study investigating your experience of online behaviour in your adolescent years. The purpose of this study is to describe the behaviours of young adults aged between 18 and 25 years old when engaging in online activities as teenagers, as well as to explore both the positive and negative experiences they had online during this time of their lives. Specifically, you have provided your contact details through a self-referral and identification process to participate in a further discussion surrounding more details of your negative experiences online, along with other self-identified peers. If you are currently feeling mentally or emotionally vulnerable, we would suggest you do not complete the survey if you think that these questions will distress you.

This project is funded by the European Commission, Directorate C-Schengen, Unit C4-Internal Security Fund (Home/2013/ISEX/AG/INT/4000005230). The project as a whole is co-ordinated by Professor Julia Davidson of the Centre for Abuse and Trauma Studies at Middlesex University (United Kingdom), with partners at Tilburg University (Netherlands), FDE Institute of Criminology and Kore University of Enna (Italy). Sample participants will be recruited from Ireland, Italy and the United Kingdom.

Should you have any questions please feel free to contact Jeffrey DeMarco (j.demarco@mdx.ac.uk) the project Research Fellow; he will be happy to provide you with any additional information you may require. All responses gathered will be treated with the greatest level of confidentiality in line with both British Society of Criminology and British Psychological Society Codes of Conduct and Ethics. The information itself will be stored in line with UK data protection guidelines. Your true identity will be known to the research team and other participants present on the day however it will be anonymised and a pseudonym will be used in all public material. During the conduction of the focus group, please know that you may withdraw at any point however, please note that once the session has terminated, it will not be possible for your data to be removed or deleted, as the researchers have no method of identifying your input from any others apart from voice recognition.

Please take the time to respond to the questions posed carefully. If you feel you do not have anything to contribute, you are not required to say anything. Your participation is greatly appreciated and will assist us in understanding the online behaviours and positive and negative experiences of young people when they go online. The discussion should take approximately 60 minutes. Please ensure you understand this Information Sheet before you agree to begin engage in the discussion and direct any further queries to Jeffrey DeMarco as indicated above.

If you agree to participate, please indicate your consent by ticking the appropriate box on the next page.

Thank you for your participation.

The ISEC Research Team

EU Online Child Safety—Victim Experience Depth Interviews

Name of Researcher:

Please tick all comments below that apply

- ☐ I confirm that I have read the information sheet provided and understand my involvement in the current study. I have been adequately and accordingly explained the details surrounding the research I am about to participate in.
- ☐ I have taken the opportunity to elaborate upon any questions I may have had.
- ☐ I have been properly provided with answers to those questions.
- ☐ I understand that my participation is voluntary and that I am free to withdraw at any time (up to completion)
- ☐ I agree that the information I give during the study can be used in any related publications, such as reports and academic articles
- ☐ It has been made clear that this study is being conducted in accordance with the guidelines of the British Criminological Association and the British Psychological Society, both my anonymity and confidentiality will be ensured

EU Child Online Safety Project
Victim Experience Online

Thank you again for participating in the current study.

The research is funded by the European Commission ISEC fund and has been developed in response to increased concern regarding the need to identify those children and young people most likely to be victimised by peers and/or adults online and to further equip both law enforcement and industry with the technological tools to enable effective preventative strategies and measures. Whilst great progress has been made in educating children about internet safety, further knowledge is needed in understanding various factors that lead to vulnerabilities, resilience and differing adult outcomes.

If you feel especially concerned about the effect participating in this study has had on you, the following services may be useful to you.

	Phone	Email	Website
Samaritans	08457 90 90 90	jo@samaritans.org	www.samaritans.org
Mind	0300 123 3393	info@mind.org.uk	www.mind.org.uk
PAPYRUS	0800 068 41 41	pat@papyrus-uk.org	www.papyrus-uk.org
Rape Crisis England & Wales	0808 802 9999	rcewinfo@rapecrisis.org.uk	ww.rapecrisis.org.uk
The Survivors Trust	01788 550554	info@thesurvivorstrust.org	www.thesurvivorstrust.org
Victim Support	08 08 16 89 111	supportline@victimsupport.org.uk	www.victimsupport.org.uk

If you would like further details about our work on the current research initiative, please visit the project site www.euchildsafetyonlineproject.com and remember to check in regularly for project updates. Additionally, you may be interested in some of our previous work related to online abuse, child exploitation and grooming behavior (www.europeanonlinegroomingproject.com) and the ROBERT online risk-taking behavior project (www.childcentre.info/robert). Further details of the team at Middlesex and associated research projects can be found on the Centre for Abuse and Trauma Studies website (www.cats-rp.org.uk).

Finally, should you have any further questions or queries related to this phase of the project or additional phases, please do not hesitate to contact either our Principal Investigator Professor Julia Davidson (j.davidson@mdx.ac.uk) or the Project Research Fellow, Mr. Jeffrey DeMarco (j.demarco@mdx.ac.uk).

Thanking you once again for your assistance and time for such an important area of research. Your involvement is greatly appreciated.

Kindest Regards,

Professor Julia Davidson and Jeffrey DeMarco

Appendix V: Work Package 2 Depth Interview schedules

Focus Group Schedule
Historical Victim Experience

The topic guide follows a funnel design, beginning with a general broad question, moving onto more structured in depth topics, and concluding with two wrap-up questions aimed to empower the participants and create a sense of closure to the session (Kreuger & Casey, 2000). These wrap up questions are designed within a communal constructivism framework, where the participants are afforded an active role in advising the younger generation about safety online.

1. **General information on technology use as a teenager (10 mins)**
   - Which devices did you use most often to go online?
   - What were the primary influencers and motivators for using these devices?
   - What did you spend most of your time doing online?
   - What were the main activities you engaged in online?

2. **Safety and behaviour online (20 mins)**
   - Where did you learn about staying safe online when you were this age?
     Prompt - school/discussions with parents/friends/TV/online indicators/other?
   - Which of these had the most/least impact on the way you behaved online?
     - Why?
   - What could have been done differently in order to make you more aware?
   - What would you do online that you knew was risky or possibly dangerous?
     Prompt - added people to friends list had never met/public profile page/downloaded illegal material, subscribed to websites, input credit card details, talked to strangers online etc.
   - What influenced you to do these things?
     Prompt talked to strangers online – liked the person, good for self-esteem, had things in common, confided in them, felt lonely, thrill, excitement, sexual experimentation

3. **Online interactions (20 mins)**
   (a) The positive aspects
   - Tell me about the positive aspects of interacting with other people online when you were this age?
     Prompts – would it benefit existing relationships/result in new friendships or relationships/help you find people you had things in common with/would you learn new things?
   - In what way?

- Why was this a positive thing to you at this age?

(b) The negative aspects

- Tell me about the negative aspects of interacting with other people online?
  Prompt – would it have a negative impact on existing relationships, would you get sent messages you didn't want to get, be contacted by people you didn't want to hear from?
  - In what way?
  - How would you have coped with this at the time?

4. Exposure to risks online (15 mins)

- Did you ever feel at-risk or in danger when you were online at this age?
  Prompt - threatening messages, *sexual messages*
- What was it about these situations which made you feel at-risk or in danger?
- How did you cope with these situations?
- Looking back, how have these situations affected you today?
  Prompt - relationships, online behaviour, friendships, well-being, fear

5. Reflections and recommendations (5-10 mins)

- Is there anything on this topic we have not discussed that you think is important to mention?
- What is the one piece of advice you would give to a teenager today about spending time online?

Appendix VI: Work Package 2 Survey

About You

1. What is your gender?

Male	Female
☐1	☐2

2. What age are you?

☐1 Under 18 → ***If respondents tick this option they will be directed to End of survey***
☐2 18
☐3 19
☐4 20
☐5 21
☐6 22
☐7 23
☐8 24
☐9 25
☐10 Over 25 → ***If respondents tick this option they will be directed to End of survey***

3. Which of the following BEST describes your ethnic or cultural background?

☐2 White or White British
☐3 Any other White Background
☐4 Black or Black British
☐5 Black—African origin
☐6 Black—Caribbean origin
☐7 Any other Black Background
☐8 Asian or Asian British
☐9 Any other Asian background
☐9 Other, including Mixed race

4. Which of these descriptions BEST describes your situation in regard to work?

In employment	☐1
In education	☐2
Unemployed	☐3
Unable to work due to long term illness or disability	☐5
Looking after the home	☐6
Other, please specify_____	☐7

5. What is the highest level of education your parents/guardians have completed to date?

	Mother/Female Guardian	Father/Male Guardian
Primary school or less	☐1	☐1
Secondary school or equivalent	☐2	☐2
College/Apprenticeship or equivalent	☐3	☐3
Sixth form (GSCEs and A levels)	☐4	☐4
University Diploma/Certificate	☐5	☐5
Undergraduate Degree	☐6	☐6
Postgraduate or Higher Degree	☐7	☐7
Don't Know	☐8	☐8

6. How would you define your sexual orientation?

Heterosexual	Gay or Lesbian	Bisexual	Unsure	Other, please specify
☐1	☐2	☐3	☐4	☐5_____

Your Life as a Teenager

Now we would like to ask you some questions about your life when you were younger, between the ages of 12 and 16 years old. Think back to this time.

7. Between the ages of 12 and 16 where did you live for most of the time?

In the United Kingdom	☐1
Other EU country	☐2
Non EU country	☐3

8. Was where you mostly lived…?

In a city	☐1
In a village	☐2
In a town	☐3
In a rural area	☐4

9. Between the ages of 12 and 16 please rate how true the following statements were for you during that time?

	Not True	Somewhat True	Certainly True
I had at least one good friend I could rely on	☐1	☐2	☐3
I lived in a neighbourhood where it was safe to go out alone in the dark	☐1	☐2	☐3
I got on well with my parents	☐1	☐2	☐3
I mostly enjoyed being in school	☐1	☐2	☐3
I thought before I did things	☐1	☐2	☐3
I did things I knew would get me in trouble	☐1	☐2	☐3
I would get very angry and often lose my temper	☐1	☐2	☐3

10. Also thinking back to this time, please rate how often you did the following?

	Often	Sometimes	Rarely	Never
Had so much alcohol I got really drunk	☐1	☐2	☐3	☐4
Played truant from school	☐1	☐2	☐3	☐4
Got in trouble with my teachers for bad behaviour	☐1	☐2	☐3	☐4

Life as a Connected Teenager

11. Between the ages of 12 and 16 which technologies did you use? Please tick all that apply.

A mobile phone	☐1
A tablet	☐2
A laptop	☐3
A desktop computer	☐4
A gaming console	☐5

12. Between the ages of 12 and 16, how often would you say you went online?

Every day/ Almost every day	Once or twice a week	Once or twice a month	A few times a year	Never
☐1	☐2	☐3	☐4	☐5

13. Between the ages of 12 and 16, consider what you spent your time doing when you were on the Internet. Please rate how frequently you did the following activities:

	Often	Sometimes	Rarely	Never
Emailing	☐1	☐2	☐3	☐4
On social networking sites	☐1	☐2	☐3	☐4
Instant messaging	☐1	☐2	☐3	☐4
Playing games	☐1	☐2	☐3	☐4
Going to chat rooms	☐1	☐2	☐3	☐4
Doing schoolwork	☐1	☐2	☐3	☐4
Virtual worlds	☐1	☐2	☐3	☐4
Listening to music	☐1	☐2	☐3	☐4
Watch videos/Movies	☐1	☐2	☐3	☐4
Other (please specify)_____	☐1	☐2	☐3	☐4

14. Between the ages of 12 and 16 where did you most often go online?

At school	☐1
At home – in a private room such as your bedroom	☐2
At home – in a shared space such as the living room	☐3
At another house (e.g. friend's, relative's, neighbour's)	☐4
At an Internet café	☐5
Other (please specify)_____	☐6

15. Also thinking back to this time, did you learn anything about Internet safety…?

	Yes	**No**
At home	☐1	☐2
At school	☐1	☐2
From friends	☐1	☐2
On television	☐1	☐2
Online	☐1	☐2

16. Between the ages of 12 and 16 how often did your parent/s ask you about what you did or where you went on the Internet?

Often	Sometimes	Rarely	Never
☐1	☐2	☐3	☐4

17. Between the ages of 12 and 16 did your parent/s have blocks or filters on your Internet access?

Yes	No	Don't Know
☐1	☐2	☐3

18. Between the ages of 12 and 16 how often did you do the following?

	Often	**Sometimes**	**Rarely**	**Never**
Gave out personal information online (e.g. my last name, the name of my school, my home address, my email address)	☐1	☐2	☐3	☐4
Downloaded pirated material (e.g. illegal films, games, music)	☐1	☐2	☐3	☐4
Added or accepted people to my friends list I had never met in person before	☐1	☐2	☐3	☐4
Visited adult pornographic sites online	☐1	☐2	☐3	☐4
Meet someone my own age face to face I had only known online	☐1	☐2	☐3	☐4
Meet an adult face to face I had only known online	☐1	☐2	☐3	☐4

19. Between the ages of 12 and 16 please rate how often the following happened in your life?

	Often	Sometimes	Rarely	Never
You were harassed or threatened face to face	☐1	☐2	☐3	☐4
You were harassed or threatened online or by text	☐1	☐2	☐3	☐4

20. Also thinking back to this time, please rate how often you did the following?

	Often	Sometimes	Rarely	Never
You harassed or threatened someone else face to face	☐1	☐2	☐3	☐4
You harassed or threatened someone else online or by text	☐1	☐2	☐3	☐4

Online Experiences as a Teenager

Teenage years for many young people are about exploring identities and becoming increasingly curious about sex. The amount of information available about sex on the Internet, and the ease with which people can communicate online means it is frequently being used by teenagers to explore this part of their identity.

21. Between the ages of 12 and 16, did you ever send someone a sexually suggestive message, or a photo or video of yourself by phone or online?

Yes	No	Don't Know
☐1	☐2	☐3

➔ ***Respondents who tick No or Don't Know to 21 will be directed to Q23***

22. Who did you send these messages, photos or videos to? Please tick all that apply.

Someone I only knew online	☐1
My boyfriend/girlfriend at the time	☐2
A friend or acquaintance from school	☐3
A friend or acquaintance from somewhere else	☐4
Someone else I was interested in getting together with	☐5
Someone I didn't know	☐6
Not sure	☐7

When online you also might get sent sexual messages by people you know, or by people you don't know.

23. Between the ages of 12 and 16 please rate how often the following happened in your life **when you were online**?

	Often	**Sometimes**	**Rarely**	**Never**
Someone asked me for sexual information about myself, e.g. really personal questions, like what my body looked like or sexual things I might have done	☐1	☐2	☐3	☐4
Someone asked me to do something sexual	☐1	☐2	☐3	☐4
Someone asked me to meet up in person to engage in sexual activity	☐1	☐2	☐3	☐4

➔ ***Respondents who tick Never to Q23 will be directed to End of Survey***

24. Who sent you these messages? Please tick all that apply.

Someone I only knew online	☐1
My boyfriend/girlfriend at the time	☐2
A friend or acquaintance from school	☐3
A friend or acquaintance from somewhere else	☐4
Someone else I was interested in getting together with	☐5
Someone else I knew	☐6
Someone I didn't know	☐7
Not sure	☐8

25. Thinking of the person or people who sent you these messages online, were they male or female?

Male/s	Some males and females	Female/s	Not sure
☐1	☐3	☐4	☐6

26. Thinking of the person or people who sent you these messages online, what age were they? Please tick all that apply. If you are not sure, please give your best guess.

5 or more years **older** than me	☐1
1 to 4 years **older** than me	☐2
Around the same age as me	☐3
1 to 4 years **younger** than me	☐4
5 or more years **younger** than me	☐5
Don't know	☐6

Did you talk to anyone about these messages you received?

Yes	No
☐1	☐2

➔ ***Respondents who tick No to Q27 will be directed to Q31***

27. Who did you talk to about these messages? Please tick all that apply.

My mum or dad	☐1
My brother or sister	☐2
A friend	☐3
My boyfriend or girlfriend	☐4
A teacher	☐5
Someone whose job it is to help (e.g. social worker, Police, GP, psychologist, etc.)	☐6
Another adult I trust	☐7
Someone else	☐8
I called a helpline	☐9
I used an online reporting mechanism	☐10

➔ ***Respondents who tick "I called a helpline" in Q28 will be asked Q29 and Q30, the others will go to Q31***

28. Which helpline did you call? _____

29. Please rate how useful this service was?

Very useful	Somewhat useful	Not very useful	Not at all useful
☐1	☐2	☐3	☐4

30. Is there anything else you would like to add about your experience of receiving these online sexual messages or requests?

31. Our study is interested in the experiences of young adults who were sent sexual messages or requests when they were online as a teenager. In order to explore this further we are conducting a series of focus groups in the near future to discuss this and the general topic of youth safety online. We would gladly welcome any input you could give us by participating in these focus groups. If you would like to get more information on these focus groups please insert your email address below and we will be in touch. Rest assured, by providing us with your email address you **are not** committing to participation. Additionally, your email address **will not** be stored linked to any other information you have provided us with in this survey.

Yes I would like to receive more information on these focus groups

_____

Appendix VII: Dissemination list

Dissemination and impact

Over the course of the project, a number of dissemination strategies have been applied as the project developed. Due to the ever-evolving area in which the research is being conducted, a diverse audience and set of stakeholders have been identified and targeted in order to communicate findings as they develop. This includes forums across academia, government, law enforcement and the third sector. Below is a list of the more substantial outputs of the project however please note that this list is not complete.

- Project website (www.euchildsafetyonlineproject.com) – developed for the purpose of the consortium and stakeholders; upkeep by management team at Middlesex. Utilised for regular updates and news, as well as information regarding the project and consortium
- Twitter (@EU_onlinesafety) – presence on social media platform, providing regular project updates and relevant news in the field
- Literature review produced (**August 2015**) surrounding collaborative practice between law enforcement and industry; executive summary provided
- London meeting for partners and advisory groups—method development and 'think tank' session with professionals—**October 2014: Senate House**
- Blog entry produced related to preliminary findings (http://mdxminds.com/2015/02/24/fostering-collaboration-between-the-police-andindustry-in-the-prevention-and-investigation-of-online-child-abuse)
- Interim Report/Project update—available on website—**January 2015**
- Europol E3 Cybercrime Meeting—Professor Julia Davidson named to cybercrime think tank; provides summary of current project—**February 2015**
- Developing research-informed good practice models in preventing online child abuse. Poster presented by Dr. Carly Cheevers at RCSI's Annual Research Day at RCSI, Dublin , Ireland—**March 2015**
- Aiken, M.P. (2015). "Cyberpsychology on a world stage." . IADT Dun Laoghaire Institute of Art Design and Technology. Dublin. Ireland—**March 2015**
- St. Mary's University, College Academic Seminar series—Professor Julia Davidson presents preliminary findings—**April 2015**
- Professor Mary Aiken participated in Public Seminar on "*Cyber Crime affecting personal safety, privacy, and reputation, including cyberbullying*." (22nd April) Law Reform Commission, President's Hall, Law Society of Ireland, Dublin, Ireland—**April 2015**
- University of Lleida, School of Law—Dr. Jeffrey DeMarco presents to faculty and students on project findings—Lleida, Spain—**April 2015**
- Annual Report—European Illegal use of the internet: Police and Industry Collaboration
- Enna meeting for partners—method development WP2 and project update— University of Kore in Enna: UKE Campus, Enna, Sicily—**May 2015**
- Online Childhood Exploitation Conference—Consortium presentations to faculty and student body. All presentations available on project website. University of Kore in Enna: UKE Campus, Enna, Sicily—**May 2015**

- GSMA Mobile Alliance presentation by Professor Julia Davidson—preliminary qualitative findings—**May 2015**
- Panel presentations at the European Dialogue on Internet Governance (EuroDig)—Dr. Jeffrey DeMarco presents findings on Youth Empowerment and Cyber-security and crime—Sofia, Bulgaria: **June 2015**
- Networking event and round table discussion on law enforcement strategies—Dr. Jeffrey DeMarco. Stockholm Criminology Symposium, Stockholm, Sweden—**June 2015**
- Panel on prevention of online childhood exploitation—Dr. Jeffrey DeMarco; UK Internet Governance Forum, London, UK: **June 2015** (withdrew due to illness)
- "Local Police National congress" - dissemination and support related to police forces survey dissemination. Dr. Elisa Corbari and Dr. Angela Centuori: World Join Center, Milano, **June 2015**
- "Gestire l'ingestibile. Le professioni di aiuto nella società del rischio" workshop for helping professionals - dissemination and support related to police forces survey dissemination. Dr. Elisa Corbari and Dr. Angela Centuori: Sala San Francesco, Ferrara, **June 2015**
- Roundtable discussion on evolving issues in cyber-crime and legal harmonisation. Dr. Jeffrey DeMarco. British Society of Criminology Annual Conference; Plymouth, UK: **July 2015** (withdrew due to illness.)
- Thematic panel on sexual crimes online: Victimisation and Policing. Professor Julia Davidson and Dr. Jeffrey DeMarco. European Society of Criminology Annual Conference, Porto, Portugal: **September 2015**
- EC Funding for Action Grants and other potential sources of funding for VSE members – Grooming project experience. Dr. Elisa Corbari and Francesca Savazzi: APAV Offices, Lisbon, **October 2015.**
- PROTEUS Seminar | Identity theft online: preventing, fighting & supporting victims – contact with speakers and dissemination. Dr. Elisa Corbari and Francesca Savazzi: Judiciary Police, Lisbon, **October 2015.**
- Industry Stakeholder Symposium, Dublin, Ireland—Entire consortium: **October 2015**
- "Tavolo di confronto e di coordinamento sulle iniziative in favore delle vittime" (Coordination working group related to victims protection) – dissemination and support related to youngsters survey dissemination. Dr. Elisa Corbari: Rome, **October 2015**
- Preliminary findings from EU Child Safety Online Project. Presentation to expert stakeholders at Symposium on Preliminary Findings from EU Child Safety Online Project, presented by Dr. Carly Cheevers at RCSI, Dublin, Ireland—**October 2015**
- Thematic panel on digital dangers: Preliminary analysis on WP1 and WP2—Professor Julia Davidson and Dr. Jeffrey DeMarco. American Society of Criminology Annual General Meeting, Washington, DC, USA: **November 2015**
- Risk factors and likelihood of youth receiving online sexual solicitations from adults – Preliminary findings from the EU Child Safety Online Project. Invited speaker at Psychology Colloquium, presented by Dr. Carly Cheevers at University of Limerick, Ireland—**February 2016**
- "Cyber Leadership" presentation by Professor Mary Aiken. UCD Women in Leadership. University College Dublin. Dublin. Ireland. **February 2016**

- Aiken, M. P. & Cheevers, C. "*Cyber Babies to Sexting Teens: The impact of Technology on the Developing Child*" Psychology Society of Ireland, Symposium - Special Interest Group for Child and Adolescent Psychology, Dublin, Ireland—**April 2016**
- Online risk and young person conference, Tilburg, Netherlands—Entire consortium. **April 2016**
- Aiken, M. P. (2015). "*Cyberpsychology of the impact of emerging technology on the developing youth.*" TEDX Talk. The High School Dublin, Dublin, Ireland—**April 2016**
- Annual Conference "Taking victim support to the next level, connect and commit" co-organised by Slachtofferhulp Nederland and Victim Support Europe, workshop "Youngsters victimization prevention: how to prevent online grooming and unsafe behaviours", Muntgebouw, Utrecht - The Netherlands, **May 2016**
- Risk factors associated with increased likelihood of youth receiving 'red flag' online sexual solicitations. Paper presented at 21st Annual Cyberpsychology, Cybertherapy & Social Networking Conference at IADT by Dr. Carly Cheevers, Dublin, Ireland—**June 2016.**
- Europol Cyber Crime Centre (EC3) Expert Seminar—presentation on victimisation by Dr. Jeffrey DeMarco, Europol, Hague, Netherlands—**June 2016**
- Final ISEC conference, invited event and presentation of findings: Entire consortium. London, UK—**June 2016**
- Annual Conference of the European Society of Criminology – Eurocrim 2016, panel "A European perspective on Challenges of Policing Online Childhood Sexual Abuse", Dr. Elisa Corbari and Dr Jeffrey DeMarco Munster, Germany, **September 2016**

Appendix VIII: Review of legal literature from participant countries

UK

English and Welsh law in combatting Online Childhood Sexual Abuse

Act and Year	Relevant Section	Title	Information
Criminal Justice Act 2003	227	Extended Sentence for Certain Violent or Sexual Offences: Bysons 18 or over	Where a person is convicted of a defined sexual offense they are liable for an extended period of imprisonment, which is not to exceed eight years.
Criminal Justice Act 2003	228	Extended Sentence for Certain Violent or Sexual Offences: Byson under 18	Minor under eighteen may be sentenced to an extended term of imprisonment, not to exceed eight years, where the crime is one of a sexual nature.
Criminal Justice and Immigration Act 2008	63	Possession of Extreme Pornographic Images	Criminal offense of possessing extreme pornographic images. An image is considered to be 'extreme' if it depicts an act which threatens a person's life, results in serious injury to a person's anus, breasts or genitals, shows interference with a corpse or depicts an act of sex with an animal. Section 67 sets the penalty for this offense at imprisonment for up to three years on conviction on indictment, or up to six months' imprisonment and/or a fine not exceeding the statutory maximum on summary conviction.
Sexual Offences Act 2003	1	Rape	A person is guilty of an offense if they intentionally penetrate the vagina, anus or mouth of another person with their penis and without the consent of the other p. Rape renders the offender liable to life imprisonment.
	2	Assault by penetration	Defines the offense of sexually penetrating the vagina, anus of mouth of another person with an object without their consent. If found guilty the term of imprisonment must not exceed life.
	3	Sexual Assault	States that it is unlawful to sexually touch another person without their consent. Sexual assault incurs a maximum sentence of ten years' imprisonment on conviction on indictment, or imprisonment for up to

		six months and/or a fine not exceeding the statutory maximum upon summary conviction.
4	Causing a person to engage in sexual activity without consent	States that a person commits an offense where they cause another person to engage in sexual activity with another person without consent, including penetration of the other person's vagina, anus or mouth. Upon conviction on indictment they face a maximum term of ten years' imprisonment; on summary conviction, the offender will be liable to a maximum term of six months' imprisonment and/or a fine not exceeding the statutory maximum.
5	Rape of a child under 13	Imposes a maximum penalty of life imprisonment for anyone who intentionally penetrates the vagina, anus or mouth of a child under the age of thirteen years.
6	Assault of a child under 13 by penetration	This section states that it is unlawful to penetrate the vagina, anus or mouth of a child under thirteen with an object. The maximum sentence for this is life imprisonment.
7	Sexual assault of a child under 13	Defines the offense as to sexually touch a child under thirteen. The maximum sentence upon conviction on indictment is a term of imprisonment not to exceed fourteen years. Upon summary conviction, the offender will be liable to a maximum term of six months' imprisonment and/or a fine not exceeding the statutory maximum.
8	Causing or inciting a child under the age of 13 to engage in sexual activity	States that it is a criminal offense to cause or encourage a child under thirteen to engage in sexual activity with another person. This includes penetration of the vagina, anus or mouth of another person. If found guilty on conviction of indictment, the offender is liable to up to fourteen years' imprisonment. Upon summary conviction, the offender will be liable to a maximum term of six months' imprisonment and/or a fine not exceeding the statutory maximum.
9	Sexual activity with a child	This section states that anyone aged eighteen or over who intentionally sexually touches a child under the age of

		thirteen, or a minor under sixteen who they do not believe is sixteen or over, is guilty of an offense. Upon conviction on indictment, the offender will be liable to up to fourteen years' imprisonment. Upon summary conviction, the offender will be liable to a maximum term of six months' imprisonment and/or a fine not exceeding the statutory maximum.
10	Causing or inciting a child to engage in sexual activity	Any adult who intentionally causes or incites a child under the age of thirteen, or a minor under the age of sixteen where they do not reasonably believe the child to be sixteen or over, to engage in sexual activity, is guilty of an offense and liable to, upon conviction on indictment, up to fourteen years' imprisonment. Upon summary conviction, the term will be up to six months' imprisonment and/or a fine not exceeding the statutory maximum.
11	Engaging in a sexual activity in the presence of a child	It is unlawful for an adult to engage in sexual activity in the presence of a child under the age of thirteen for the purposes of sexual gratification. The same applies if the child is under the age of sixteen and the offender does not reasonably believe the child to be sixteen or over. Upon conviction on indictment, the maximum term of imprisonment is ten years; upon summary conviction, offender will be liable to a maximum term of six months' imprisonment and/or a fine not exceeding the statutory maximum.
12	Causing a child to watch a sexual act	It is a criminal offense to cause a child under the age of thirteen, or a minor under sixteen who they do not believe to be sixteen or over, to watch a person engage in sexual activity for the purposes of obtaining sexual gratification. This is punishable by up to ten years' imprisonment on conviction on indictment, or up to a maximum term of six months' imprisonment and/or a fine not exceeding the statutory maximum on summary conviction.
13	Child sex offences committed by children or young people	where a minor under the age of eighteen commits any offense under sections 9 - 12, on conviction on indictment they may be sentenced to up to five years'

		imprisonment, or up to a maximum term of six months' imprisonment and/or a fine not exceeding the statutory maximum on summary conviction.
14	Arranging or facilitating the commission of a child sex act	It is an offense to arrange or facilitate the commission of an act that is against the law under sections 9 - 13. On conviction on indictment, the offender will be liable to up to fourteen years' in prison; on summary conviction, the maximum penalty is six months' imprisonment and/or a fine not exceeding the statutory maximum.
15	Meeting a child following sexual grooming, etc.	Having communicated with a child under the age of sixteen on at least two previous occasions, arranges to meet them with the intention of committing a crime under sections 9 - 13, is guilty of an offense. This is punishable by up to ten years' imprisonment on conviction on indictment, or up to six months' imprisonment and/or a fine not exceeding the statutory maximum on summary conviction.
16	Abuse of position of trust: Sexual activity with a child	Up to five years' imprisonment for anyone who abuses a position of authority to engage in sexual touching with a child under the age of thirteen or where the minor is under eighteen and the offender does not believe that they are eighteen or over. On summary conviction, the maximum penalty is six months' imprisonment and/or a fine not exceeding the statutory maximum.
17	Abuse of Position of Trust: Causing or Inciting a Child to Engage in Sexual Activity	Encouraging a child to engage in sexual activity when the offender is in a position of trust renders the offender liable to the same penalties as set out in section 16.
18	Abuse of Position of Trust: Sexual Activity in the Presence of a Child	Byson in a position of authority engages in sexual activity in the presence of a child they commit and offense, the same penalties as laid out in section 16 will apply
19	Abuse of Position of Trust: Causing a Child to Watch a Sexual Act	Up to five years' imprisonment for anyone who abuses a position of authority to cause a child to watch a sexual act where the child is under thirteen or where the minor is under eighteen and the offender does not believe that they are eighteen or over. On summary conviction, the maximum penalty is six months' imprisonment

		and/or a fine not exceeding the statutory maximum.
47	Paying for Sexual Services of a Child	Anyone who obtains the sexual services of a child under the age of thirteen for a financial reward to the child or a third person is guilty of an offense. Where the act includes the penetration of the child's vagina, anus or mouth with a body part or any object, the sentence will be life imprisonment. Where the minor is under the age of sixteen the penalty will be up to fourteen years' imprisonment if the offense includes penetration, or in any other case up to fourteen years' upon summary conviction, or up to six months in addition to a fine up to the statutory maximum upon conviction on indictment. If the child is under eighteen and the offender does not reasonably believe the child to be eighteen or over, he/she will be liable to imprisonment for up to seven years on conviction on indictment, or up to six months in addition to a fine up to the statutory maximum on summary conviction.
48	Causing or Inciting Child Prostitution or Pornography	Against the law to incite a child under thirteen or under eighteen, whom the offender does not believe is over eighteen, to engage in pornography. Those guilty under this section face up to fourteen years' imprisonment on conviction on indictment, or up to six months in addition to a fine up to the statutory maximum on summary conviction.
49	Controlling a Child Prostitute or a Child Involved in Pornography	An offense to intentionally control the activities of a child under the age of thirteen, or under eighteen if the offender does not believe reasonably believe the child to be aged eighteen or over, relating to prostitution or pornography. This renders the offender liable to imprisonment for up to fourteen years on conviction on indictment, or up to six months, in addition to a fine up to the statutory maximum upon summary conviction.
50	Arranging or Facilitating Child Prostitution or Pornography	Penalty of imprisonment not to exceed fourteen years for anyone who arranges or facilitates the participation of a child in pornographic activity if the child is under the age of thirteen, or under

			eighteen and the offender does know the minor is under age. On summary conviction, the penalty is up to six months' imprisonment and a fine not exceeding the statutory maximum.
	66	Exposure	Exposes their genitals with the intent that someone else sees them, they are guilty of an offense and may be sentenced to up to two years' imprisonment on conviction on indictment, or up to six months' imprisonment and a fine not exceeding the statutory maximum on summary conviction.
	67	Voyeurism	Observe another without the other person's consent for the purposes of sexual gratification. It is equally unlawful to operate equipment to enable another person to commit the offense above, or to record another person doing a private act without consent for the purpose of sexual gratification. This is punishable by imprisonment for up to two years on conviction on indictment, on summary conviction the penalty is up to six months' imprisonment and a fine not exceeding the statutory maximum.
Protection of Children Act 1978	1	Indecent Photographs of Children	Offense for any person to take, make, distribute, show, publish or possess (with a view to distribute) any indecent images of a child. Section 5 (Forfeiture) states that any images seized under this Act may be ordered to be forfeited by the courts. Section 6 (Punishment) states that anyone convicted under this Act may be sentenced to a maximum of ten years' imprisonment on conviction on indictment, or up to six months' imprisonment and a fine not exceeding the prescribed sum by the Magistrates' Courts Act.
Obscene Publications Act 1959	2	Prohibition of Publication of Obscene Matter	Anyone who, whether for gain or not, publishes an obscene article will be liable to imprisonment for up to five years on conviction on indictment, or up to six months' imprisonment and/or a fine not exceeding the statutory maximum on summary conviction.
Malicious Communications Act 1998	1	Offence of sending letters etc., with intent to cause distress of anxiety	Offense to send an indecent, offensive or threatening letter, electronic communication or other article to another person. The penalty under this section is up to six months' imprisonment and/or a fine not

			exceeding level 5 on the standard scale.
Protection from Harassment Act 1997	1	Prohibition of harassment	It is a crime to pursue a course of conduct which amounts to a harassment. The maximum sentence for this behaviour is six months' imprisonment and/or a fine not exceeding level 5 on the standard scale.
	4	Putting people in fear of violence	Where the victim is placed in fear of violence as a result of the harassment the maximum sentence increases to five years' imprisonment.
Criminal Justice and Public Order Act 1994	84	Indecent pseudo-photographs of children.	If the impression conveyed by a pseudo-photograph is that the person shown is a child, the pseudo-photograph shall be treated as showing a child and so shall a pseudo-photograph where the predominant impression conveyed is that the person shown is a child notwithstanding that some of the physical characteristics shown are those of an adult
	85	Arrestable offences to include certain offences relating to obscenity or indecency	Two new offences: (1) publication of obscene material and (2) creating, distributing, showing, possessing with intent to show or distribute, or advertise the distribution or showing, of indecent photographs of pseud-photographs of children.
	86	Indecent photographs of children: sentence of imprisonment.	Imprisonable and up to maximum of six months on summary convictions
Coroners and Justice Act 2009	62	Possession of prohibited images of children	Offence of possession of a prohibited image of a child, punishable by up to three years' imprisonment
	69	Indecent pseudo-photographs of children: marriage etc	As above, with non-images.
Serious Crime Bill 2014	66	Possession of paedophile manual Sexual communication with a child Changes the terminology in the SOS 2013 – child pornogrpahy and prostitution to be referred to as child sexual exploitation	Illegal the possession of written material containing advice and instructions on how to commit sexual offences against children. There will be a three year maximum sentence associated.

The Netherlands

On October 15th 2012, the Dutch Minister of Security and Justice (Ivo Opstelten) sent a letter to the Dutch Parliament expressing the intention to draft a new cybercrime legislation in the Netherlands to fight against cyber criminals (http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2012/10/15/wetgeving-bestrijding-cybercrime.html). The aim of the new legislation is to fine tune the Dutch legal framework to the needs of the services and organizations responsible for the investigation and prosecution of cybercrime. Based on technical experiences explained in the 2011 and 2012 Cyber Security Assessments, about the legal framework for cyber security, this concerns the following topics;

1. Remote entry of automated works (computers), and the placement of technical devices (software) for the purpose of investigation of severe forms of cybercrime;

2. Remote search of databases that is accessible from an automated work (computer), regardless of the location of the automated work on which the data is stored and taking into consideration agreements and rules of international legal assistance;

3. Making data inaccessible from an automated work (computer), regardless of the location of the computer on which the data is stored; taking into consideration the agreements and rules of international legal assistance;

4. Criminalization of the trade in stolen (digital) data.

The Dutch national and international power and measures to act against cybercrime offenses are decreasing as a result of the cross-border nature and the emergence of so-called cloud computing. It also appears that the industrial self-regulation malfunctions and those offenses that could be prevented through better and earlier technical measures often still occur. An important issue is the impossibility to trace criminal internet activities because it is relatively easy for cybercriminals to prevent their digital tracks from being monitored, for example by the use of software to encrypt data and delete their communication paths.

According to international law, (digital) investigative actions on foreign terrain can only take place through international legal assistance. As shown above, it is not always possible to determine where data is located. If that is the case, the police and public prosecution service must be able to continue their investigation under the conditions outlined below.

(1) Remote entry of automated works (computers) and placement of technical means (software) for investigative purposes of severe forms of cybercrime

In paragraph 1, the development toward the use of more mobile Internet is explained. Also the increasing use of the encryption on computers is explained. The police and the public prosecution service indicate that various forms of crime exist which are hidden from their view because the police does not have enough power to invade a computer. Article 125i of the Dutch Code of Criminal Procedure offers the legal possibility for investigators to search a

place to record data that are stored or recorded at that place on a data server. From parliamentary history, we can infer that it is not permitted that an automated work, such as a computer, is penetrated remotely for the purpose of investigation of serious forms of cybercrime. This concerns both remote entering for the purpose of wiretapping confidential communication, and remote entering for searching an automated work. In order to get access to this data for the purpose of investigation of serious forms of cybercrime, it is necessary that software can be secretly installed that allows the encryption of the data to be undone or circumvented.

In the light of technological developments, a statutory legal power should be established for remotely penetrating an automated work concerning the above purposes. The changed circumstances warrant the inclusion in the Dutch Code of Criminal Procedure of a specific authority to remote intrusion of an automated work for the investigation of serious forms of cybercrime.

(2) Remote search of data that is accessible from an automated work (computer), regardless of the location of the automated work on which the data is stored and taking into consideration agreements and rules of international legal assistance

In paragraph 1, the example of a botneck was provided that gives the cyber criminal the opportunity to move his data around the world very fast. This method is increasingly common. Recently, cyber criminals are aware of the fact that the police is attempting to access their networks and data, and take measures against that to prevent police investigation. Usually, the data are moved very fast around the global internet or the paths to enter the data are changed.

Criminal groups also often take measure to detect whether third parties, such as the police or others, are attempting to access their files. When they detect such signals, they protect their data by moving their data files with images for example as fast as possible, and do not hesitate to fight against (legal) intruders using digital means. These technological developments make it very difficult to determine the location of the stored data and the fact that location of the stored data changes often.

Where in the past most data was stored on one's own computer or on a separate data server, data is now stored via the internet on a server in another country or in the cloud. The starting point is that criminal investigation can only be exercised on one's own territory. To perform investigative actions on the territory of another state, international legal assistance is required. The opposite also applies: if a foreign state wants to conduct investigative actions on the Dutch territory, they also require official legal assistance (article 552h, the Dutch Code of Criminal Procedure). However, the time delays because a request for legal assistance is necessary, works negatively against cybercrime investigation and limits the effectiveness of official legal assistance.

The Cybercrime Convention of the Council of Europe (Vatis, 2010) has a provision on remote access to computer data regardless of the location of that data (article 32). This access is

limited to publicly accessible data and other data on the condition of consent of the rightful claimant. The Cybercrime Convention does not have provisions on the gathering of data that are not publicly accessible without consent of the rightful claimant, meaning the official legal assistance is required. However, as argued above, in the remote search of computers, in practice, it's not always possible to determine the exact location of the data. A request for official legal assistance is therefore impossible in that case.From the perspective of effective investigations, it is of vital importance that data can be retrieved regardless of the location where they are stored. Therefore, the police and the public prosecution service insisted on relevant legislation. In this relevant legislation, following principles are important. If knowledge is available about the location of the data, and the data are located on a foreign server, a request for legal assistance is designated. If there is no knowledge about the location of the stored data, they should for obtaining evidence be able to be searched and taken over. The Belgian Code of Criminal Procedure also stipulates that during the search of an automated work, data can be taken over. When it turns out that the data are not located on Belgian territory, the data are only copied and the foreign state is notified.

(3) Remotely making data inaccessible that is accessible from an automated work (computer), regardless of the [geographical] location of the automated work on which the data is stored, and taking into consideration agreements and rules of international legal assistance

A special aspect is the power to make data found during remote search of an automated work inaccessible. In the Netherlands, the possibility currently exists that, when a place is entered to record data that is stored on a data server at that place, and when the data is or was used for committing a crime (such as child pornography), the data are rendered inaccessible to end the crime (article 125o, Dutch Code of Criminal Procedure). In addition, it is desirable that during the introduction of the police to remotely intrude an automated work, such as a computer, also a power is created to render such data inaccessible. After all, it is possible that during a remote search, child pornography is found. This was the case during the aforementioned investigation that the THTC performed on child pornographic images on servers in the Tor-network where the police found very harmful pornographic material that was stored in an encrypted form on a server. In absence of knowledge about the location of the storage of the data, it is impossible to search for legal assistance because nobody can be addressed while the crime continuous. The severity of the crimes can require that the data are immediately rendered inaccessible. This can entail that the data is deleted, and therefore, it is desirable to establish a legal power to make data inaccessible or to erase data found during remote searches of an automated work. This is in line with the provisions of article 125o of the Dutch Code of Criminal Procedure. Here, again, it applies that if knowledge is available about the location of the data, a request for legal assistance must be addressed to the authorities of the foreign state.

(4) Criminalization of the trade in stolen (digital) data

On the internet, offenses are committed where data is gathered via hacking or other means that are of interest to third parties for the use in crime. Examples of this are personal data in

databases that have been compromised and that can be used to, for example, buy goods on the internet. Also, credit card data that were gathered via phishing are offered and sold on the internet.

Although, in the latter example, the use of this data to make credit cards is already punishable by law, the holding, transferring and buying this data is not punishable. This complicates investigations. The requirement to wait until the data is actually used to commit crimes implies that it is not possible to act to prevent crimes. That is certainly not reassuring to citizens and in fact a bad signal because this form of trade in stolen items would be permissible in digital form. The trade or selling of such data has developed into a separate form of crime on its own.

That trade of stolen data is currently not punishable is related to the fact that computer data, based on jurisprudence, can only be considered in specific circumstances to be goods in the meaning of articles 310 and 416 of the Dutch Criminal Code. This is relevant when data is outside the disposal of the holder and represent economical trade value. From this, it follows that copying the holder's data is not punishable because the holder retains the disposal of the data. For the involved victims, it is unacceptable that the current legislation results in unwanted gaps in cyberspace and it are desirable to make these offenses punishable.

Republic of Ireland

In the Republic of Ireland, currently the most relevant piece of legislation applicable to the issue of online sexual crimes against children is the Child Trafficking and Pornography Act (1998). Of note in this legislation is that the definition of child pornography, and the description of media through which child pornography is represented is broad enough to account for anything stored, created or accessed using Information and Communication Technologies (ICTs). This act makes it an offence to engage a child in, or allow a child to be engaged in, the production of pornography, as well as to be involved in producing or distributing such material. The maximum sentence associated with these offences is 14 years imprisonment following conviction on indictment. Possessing child pornography is also considered an offence, with an associated maximum sentence of five years imprisonment.

Unfortunately, at present in the Republic of Ireland there is no legislation dealing specifically with the act of grooming a child for sexual purposes, either on- or offline. However, there are several pieces of legislation addressing potential stages of a grooming process which can be used to prosecute an offender. Firstly, Section 10 of the Non-Fatal Offences Against the Person Act (1997) outlines that an individual who persistently communicates with another person *by any means*, impinging on their “peace and privacy or caus[ing] alarm, distress or harm to the other” is guilty of an offence. In this situation, the offender can be liable to a maximum sentence of seven years in prison. Additionally, under Section 13 of the Post Office Amendment Act (1951) (as amended in 2007) it is an offence to send “by telephone any message that is grossly offensive, or is indecent, obscene or menacing”. This offence holds a maximum sentence of 5 years in prison. Of concern with this section of legislation is that it only captures communication via the telephone. Accordingly, the Irish

Law Reform Commission and a recent report from the Internet Content Governance Advisory group in Ireland have both recommended that this be amended to also include electronic communications (Department of Communications, Energy and Natural Resources, 2014; Law Reform Commission, 2014). Finally, an amendment to the Child Trafficking and Pornography Act (1998) in 2007 posited that any Irish citizen or individual who is ordinarily resident in the State who, within or outside the country:

> *'…intentionally meets, or travels with the intention of meeting, a child, having met or communicated with that child on 2 or more previous occasions, and (b) does so for the purpose of doing anything that would constitute sexual exploitation of the child, shall be guilty of an offence and shall be liable on conviction on indictment to imprisonment for a term not exceeding 14 years…'*
>
> *(Child Trafficking and Pornography Act, 1998)*

While this legislation does capture a possible stage of the online grooming process, unfortunately it is at a high risk juncture.

Evidently, the Irish legislation in dealing with online child abuse material is more comprehensive than legislation around other forms of online sexual exploitation. It is hoped that this fragmented legislation in relation to online sexual abuse of children will be resolved with the passing of a recently introduced bill by the Irish Government. The Criminal Law (Sexual Offences) Bill (2014), if passed, will offer important laws relating to online sexual crimes against children. The bill proposes a host of new offences with maximum sentences of 10 to 14 years imprisonment, including soliciting or even attempting to solicit a child for the purpose of sexual exploitation, inviting a child to participate in sexual touching, engaging in sexual activity in the presence of a child, and causing a child to watch sexual activity, or exposing them to imagery of sexual activity. Crucially, there is a specific section in this bill making it an offence to use ICTs to facilitate the sexual exploitation of a child - again with a maximum sentence of 14 years imprisonment if convicted on indictment. The proposed bill also includes penalties for another typical stage of the grooming process, that is, the sending of sexually explicit material to a child. In this case, an individual who sends indecent imagery or messages to a child can be liable to a maximum prison sentence of five years.

The Criminal Law (Sexual Offences) Bill (2014) also proposes stricter conditions and stronger sanctions for a number of the pre-existing offences relating to online sexual crimes against children. In relation to the definition of a 'child' in association with pornographic material, the bill proposes to increase the current age limit of children from under 17 to under 18 years old. In addition, it suggests that it should be an offence to *attempt* to possess child pornography. With regard to the current offence of travelling to meet a child with the intention of sexual exploitation, an individual can only be convicted if they have communicated with the child on at least two occasions. The new bill proposes this be changed to only having communicated with the child once, and in addition makes it an offence to *make arrangements* to travel to meet a child for this purpose.

Before this bill can become law it needs to pass through the two Houses of the Oireachtas, firstly Dáil Éireann and then Seanad Éireann. Importantly, passing the Criminal Law (Sexual Offences) Bill

(2014) would address the criminal law elements of the EU directive 2011/92/EU on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, and put Ireland in a position to ratify the optional protocol to the United Nation's Convention on the Rights of the Child (UNCRC) on the Sale of Children, Child Prostitution and Child Pornography and the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Abuse (Department of Justice and Equality, 2014; Fitzgerald, 2012).

The first Irish governmental policy to focus exclusively on children was the National Children's Strategy, published in 2000 (Government of Ireland, 2000). This policy committed to improve the lives of children in Ireland and was informed by the obligations outlined by the UNCRC. Two of this policy's main objectives were that in Ireland "Children will be safeguarded to enjoy their childhood free from all forms of abuse and exploitation" and "Children will have opportunities to explore information and communication technologies in ways which are safe and developmentally supportive" (Government of Ireland, 2000, p.46). Despite an acknowledgement of the dangers of technology, there were no actions specified in this policy dealing directly with the issue of online child sexual abuse, yet it did outline initiatives to deal with broader and structural issues pertaining to all forms of child abuse and general considerations associated with children's interaction with technology. A review of the implementation of this policy concluded that by 2010 some progress had been made in most of these initiatives (Children's Rights Alliance, 2011).

On a positive note, the current national policy framework in place for children and young people until 2020, 'Better Outcomes, Brighter Futures' specifically acknowledges the role of technology in enabling the proliferation of child pornography and the threat to children from online grooming (Government of Ireland, 2014). Accordingly, the government makes a commitment to "Support all efforts, including EU and international efforts, to combat child sexual abuse, exploitation and trafficking in all contexts, including through support for an online filtering system in relation to blocking online child abuse material" (Government of Ireland, 2014, p. 81). Furthermore, it commits to assist in limiting children's exposure to age-inappropriate online material, and to promote best practice for social media providers regarding privacy and reporting of abuse.

The content of this policy framework is indicative of the increased awareness by the Irish government of the need to put the issue of child safety online at the forefront of the national agenda. Effective implementation of the policy actions outlined and the passing of the Criminal Law (Sexual Offences) Bill (2014) into law would greatly improve the situation Ireland of protecting children from online sexual abuse.

Italy

The Italian law dated October 1, 2012, n. 172, entitled "Ratification and implementation of the Council of Europe Convention for the Protection of Children against Sexual Exploitation and Sexual Abuse, made in Lanzarote October 25, 2007, and adaptation of internal rules", published in the Italian Republic Official Gazette n. 235 dated 8 October 2012, outlines two new types of offenses: incitement to practice pedophilia and child pornography (art. 414-bis), and the solicitation of minors (art. 609-undecies c.p.), otherwise known as child-grooming. The locution "child-grooming" indicates

the set of behaviours voluntarily undertaken by an adult to elicit sympathy in the child, steal his or her trust and establish an emotional type relationship, reducing the child's defenses and self-control with the aim of carry out sexual acts and/or exploitation of the child. In the light of the Council of Europe Convention on the Protection of Human Rights, the term "grooming" refers to the behaviour of the adult talking to a child or performing other actions to meet him, with the intent to commit a crime (sexual abuse, prostitution) or organize pornographic performances.

Regarding under-cover investigations, Italy boasts a wide range of action. In Italy, the Postal and Communications Police, which is a special area of the State Police that deals with computer crimes and the protection of the communications, is in charge of the under-cover investigations. With the law n. 38 of 2006, the National Centre for the Fight against the online Child Pornography was in fact established, and it has the aims of both coordinating the fight against online child pornography and investigating on it. Specifically, the areas of expertise of the Centre are: the coordination of investigations, the analysis of computer crimes, the Web monitoring and the black list management, the analysis of child pornography images. As for the situation in France, the investigative actions for fighting the phenomenon of online pedophilia are attributed to the police system at both central and local levels.

Appendix VIIII: Approved Ethics Forms

*Please read the **MU Code of Practice for Research: Principles and Procedures**[i]. The purpose of this form is to help staff and students in their pursuit of ethical research methodologies and procedures. Students should complete this form in consultation with their supervisors. The **supervisor is responsible for submission**[ii] of this form and required accompanying documents*[iii]*.**No fieldwork should begin until your Research Ethics Committee (REC) has given approval**.*

Section 1 – Applicant details

1.1 Details of Principal Investigator/Supervisor[iv]		
1.1aName: Julia Davidson	1.1b Department/Position: Professor of Criminology/Co-director CATS	
1.1c Qualifications: PhD	1.1d Email: j.davidson@mdx.ac.uk	1.1e Tel: N/A
1.2 Details of Student Researcher (if applicable)		
1.2a Name:	1.2b Programme of study/module:	
1.2c Qualifications:	1.2d Email:	1.2e Tel:
1.3 Details of any co-investigators (if applicable)		
1.3aName: Ciaran McMahon	1.3b Organisation: Cyberpsychology Research Centre, Royal College of Surgeons, Dublin, Ireland	1.3c Email: ciaranmcmahon@rcsi.ie
1.3eName: Angelo Puccia	1.3f Organisation: FDE Institute of Criminology	1.3g Email:criminologia@istitutofde.it
1.3f Name: Stefan Bogaerts	1.3g Organisation: Tilburg University	1.3h Email:s.bogaerts@tilburguniversity.edu mailto:criminologia@istitutofde.it
1.3i Name: Adriano Schimmenti	1.3j Organisation: Kore University of Enna	1.3k Email: adriano.schimmenti@unikore.it
1.4 Details of External Funding European Commission, Directorate C-Schengen, Unit C4—Internal Security Fund Home/2013/ISEX/AG/INT/4000005230 2 years Euro 593, 953. 18.		

Section 2 – Details of proposed study

2.1 Research project title	**Developing Research Informed Good Practice Policing and Industry Collaborative Models in Preventing Online Child Abuse and Profiling Child Victims**		
2.2 Proposed start date	August 1st 2014	**2.3 Proposed end date**	August 1st 2016

2.4 Main aims of the study

The project seeks to draw together the existing, recent evidence base on offender online behaviour including online grooming and accessing indecent child images, and identify policing and industry best practice in prevention. The project will ultimately seek to promote cooperation between law enforcement and industry in developing and disseminating good practice models in this area, thus promoting greater online safety for children and young people. The project will seek to explore current industry practice and law enforcement-industry cooperation aiming to produce good practice models and guidelines. The outputs will have wide relevance beyond the EU. In endeavouring to identify possible grooming behaviour as early as possible, we propose to include a study of victimology, which would involve not only the groomer but also the potential groomed. As such, using cyberpsychological research and methodology, we propose to include a virtual behavioural typology project. This project recognises, the continuum between a host of problem behaviours online, including but not limited to cyberbullying, trolling, flaming, cyberstalking, sexting, online sex offending and grooming. The project will rely on an evidence base in computer-mediated communication, cyberpsychology, network science and cyber aspects of evolutionary game theory, in order to develop a tool for law enforcement and industry to identify potential victims of grooming. Such a resource relies firstly on risk analysis of real-world victim profiling, secondly on forensic cyberpsychology aspects in virtual contexts, and thirdly on future-pacing those insights with emerging technologies for the purposes of on-going instrument development and refinement. It is consequently anticipated that these learning's can be applied equally in any existing or forthcoming social platform.

2.5 Details of data collection methods (e.g., interviews, questionnaire, observation etc.) and/or secondary data sources(e.g., UK National Statistics) to be used in the research

Due to the scale of the project and the multi-disciplinary nature, mixed methodologies will be applied throughout.

(1) Scoping Study—Literature and policy review to be undertaken. Exploration of current and recent research and policy in the online victimisation and offending area, semi-structured interviews with key stakeholders/practitioners who work with young victims of online abuse and convicted offenders, small sample drawn from partner countries. The aim of the interviews is to explore policing practice and industry in preventing online child abuse and to inform the development of the interview survey instrument to be used in stage two of the research.

(2) Survey of Industry and Law Enforcement, case studies of practice—Survey (structured) interview of sample of large police forces in partner countries and via Interpol for reach beyond EU, survey vis IPES for wider reach to police forces. UKCCIS data as baseline on industry practice plus case studies with key organisations (Facebook, Twitter, and Google plus structured interview survey of smaller companies) to explore online child protection practice including standard measures, current data capture on problems and complaints, measures taken to prevent access to images (Search engines) and to detect grooming.

(3) Virtual focus groups with self-selected youth who have experience of cyber-grooming—Using

careful and varied means of participant recruitment, a sample of 12- to 18-year-olds who report having been targeted by online predators, a virtual focus group methodology will attempt to establish a subjective phenomenology of cyber-grooming within a naturalistic context – i.e. asking victims about their experience within an environment similar to that experience.

(4) Trial of the resulting cyber-victim typology/profiling tool with law enforcement and industry partners.

Project progress will be closely monitored by the Management Group.

Section 3 – Initial Checklist to be completed by ALL applicants *Indicate your response*

3.1 The research[v] **DOES NOT involve human participants**[vi] or **animals**(or **animal by-products**)[vii] or any activity that might **cause damage** e.g., to the **environment or precious artefacts** i.e., the research involves **analytical** or **simulation modelling,** or is a **literary**, **historical or theoretical project** relying on sources available in the **public domain**[viii] and **does not** make use of **personal** or **personal sensitive data**.	Agree	**Disagree X**
3.2 The research involves **secondary data analysis**[ix] where the researcher can provide evidence that they have the necessary **approval to access*** the data *(*please provide evidence of approval)* and **DOES NOT involve** access to records of **personal or sensitive information** concerning **identifiable individuals**, or **research which may involve sharing of confidential information beyond the initial consent given**. *If there is data linkage or it may be otherwise possible to identify participants, please complete all sections of this form and **the Data Protection Act Checklist for Researchers**.*	**Agree X**	Disagree
3.3 The research **already has ethical approval from another UK Ethics Committee*** (e.g., a UK HEI or organisation e.g., NHS, IRAS[x]) and the liability insurance is provided by the other body/institution[xi]. *(*Please provide evidence of ethics approval)*	Agree	**Disagree X**
3.4 The **outputs from research** (e.g., products, guidelines, publications etc.) are **not likely to cause harm to others**, and are **in-line with UK legislation**[xii].	**Agree X**	Disagree

If you have answered **AGREE** to statements 3.1 or3.2 or3.3, and in all cases 3.4,please complete **Section 8** and **sign the declaration in Section 9. Otherwise, please complete the remainder of this form UNLESS your research involves Human Tissue (including blood)**[xiii] **then please complete the Natural Sciences REC form**[xiv] **or involves psychological research and requires approval from the Psychology REC and completion of the Psychology REC form.**

Section 4 – Research data sources and participants *Indicate your response*

4.1 Secondary data research *(e.g., published data, archives, court reports, hospital records, case notes, internet site etc.)* Please **specify data set** to be used and **how it will be obtained** and whether appropriate or required **permission** will be obtained: A document has been produced highlighting the academic data pools, data bases, websites and literary sources that will be accessed over the course of the literature and policy review for the project. These include: PsycInfo/PsycARTICLES, Web of Science, Academic Search Premier, HeinOnline, LexisNexis, Criminal Justice Abstracts, IBSS, Google scholar, Ethos, RAND, JRF, Barnados, NSPCC, Google, Home office and other gov websites (gov.uk, legislation.gov.uk, justice.gov.uk, MoJ-AS), NCJRS, Research gate, GreyNet, CIAONet (for full text pdf's only) and www.childcentre.info/robert/database. This may still be expanded through exploration of the available material and discussion with colleagues, advisors and partners. In particular, partner countries will need to investigate individual policy and grey literature independently and this will follow the auspice of what is located in this document. The majority of the material will be accessed via the internet, using access provided by Middlesex University and collaborators. Where access is not immediately available, this will be sought through the appropriate channels such as request forms, library loans and individual contacts and networks. When and if necessary, appropriate permission will be obtained.	YES
4.2Primary data from human participants: Please specify categories of human participants:*(e.g., students; those in an unequal relationship (e.g., your own students): general public; specific group(s) or team(s).(Note: NHS patients, and/or their relatives/carers, vulnerable adults unable to give informed consent must be reviewed by NHS NRES via the IRAS system. Collecting data from under-16yr olds and vulnerable adults will require DBS see 6.11)* i) **Categories and number** of participants: Project participants will include a stakeholder group of police officers from Ireland, the UK, Belgium and Italy (10 from each country), and a further survey of law enforcement in each of the partner countries (2000- 500 in each) and 2000 children and young people (500 from each country) aged 12-16. A further sample of 50 children will participate in focus groups. A case study approach to exploring industry practice will be used with key organisations including Facebook, who have recently introduced an anti-grooming tool and who work pro-actively with the police, Google and Twitter. ii)How will participants be **recruited?**(e.g., using the internet, posters, letters of introduction etc) or **access** gained to groups of participants (e.g., through gatekeepers, e.g., organisations, managers, parents, schools etc)*Please provide details:* This will be the responsibility of individual partners and decided upon through dialogue with the advisory board and partners. In general, partners will be expected to use their conacts for access following agreed upon direction with the team. iii) Details of **materials** to be used/**resources** required for this study: *(Please provide copies of questionnaires, indicative*	YES

interview questions, visual images etc. to be used in this research) The focus group schedules; surveys and all secondary material (information sheets, debriefing sheets, and consent forms) have yet to be constructed. These will on-going elements worked on throughout the duration of the project. The appropriate documents will be forwarded to the ethics board for approval as the project and instruments develop. The information packages including information sheets, consent forms, draft schedules and surveys and debriefing forms for the stakeholder guided interviews are attached in appendix B; the industry case studies in appendix C; and the survey in appendix D (NOT YET PROVIDED).	
4.3Animals or the use of animal by-products[xv]**:** If the research involves the participation and/or observation of animals or the use of animal by-products please refer to the *MU Statement on the Use of Animals in Research* and provide the following details: i) Type of animal/animal by-product ii) Justification for use of animal/animal by-products(s) iii) Where data collection is being undertaken iv) Where animals/by-products are kept and care/storage facilities v) Evidence of relevant license/permissions (where applicable)	NONE
4.4 Other data sources to be collected/used not categorised above *e.g., flora/foliage, minerals, precious artefacts etc*. Please provide details: i) Type of data ii) Justification for use iii) Where data collection is being undertaken iv) Where the data will be kept and care/storage facilities v) Evidence of required license/permissions (where applicable)	NONE

Section 5 –Anonymity, confidentiality and consent for primary and secondary research *Indicate your response*

5.1 Will the research involve collecting or analysing **personal data or sensitive personal data**? *(i.e.,personal data refers to information that may identify individuals e.g., name, address, date of birth, opinion, specifc event, set of characteristics that would clearly identify individuals or very small groups. Sensitive personal data refers to racial or ethnic origin, political opinion, religious beliefs, trade union membership, sexual life, physical or mental health, criminal matters.)* ***If 'yes'****, consider irreversibly anonymising data, if possible, by removing names and other linked or identifying information which may still identify an individual without their name. Alternatively, if personal or sensitive personal data is required for the research, you* ***must comply with the Data Protection Act (DPA)(1998)*** *and understand your responsibiities under the DPA and have received* ***data protection training****. Please complete the* ***Data Protection Act Checklist for Researchers***	**Yes X**	No	NA
5.2 Will lists of identity numbers/codes or pseudonyms for individuals and/or organisations (i.e., **linking keys to personal identifiers**) be stored securely and separately from the research data and destroyed after the study to	**Yes X**	No	NA

avoid any risk of confidentiality being compromised? *If 'no' please provide details:*			
5.3 Will you tell participants that their data will be treated **confidentially** and the **limits of anonymity** will be made clear in your **Participant Information Sheet***?(e.g., their identities as participants will be concealed unless prior consent is given to include the name of the participant in any documents resulting from the research.)*If 'no' please provide details:*	**Yes X**	No	NA
5.4 Will you obtain **Written Informed Consent*** directly from research participants (if applicable)?*If 'no' please provide details:*	**Yes X**	No	NA
5.5 Will you obtain **Written Informed Consent*** directly from gatekeepers (if applicable)?*If 'no' please provide details:*	**Yes X**	No	NA
5.6 Will consent be obtained if the research involves **sharing of data or confidential information beyond intital consent** given? *If 'no' please provide details:*	**Yes X**	No	NA
5.7 Will you inform participants that their participation is **voluntary** and that they have a **right to withdraw** from the research at any time?*If 'no' please provide details:*	**YesX**	No	NA
5.8 Will you have a process for managing **withdrawal of consent**? *If 'no' please provide details and any further actions to be taken:*	**Yes X**	No	NA
5.9 Will it be necessary for **participants to take part in the studywithout their knowledge and consent** at the time, or by **deception**e.g., covert observation? *If 'yes', please provide justification and details of how this will be managed to respect the participants/third parties involved to respect their privacy, values and to minimise any risk of harmful consequences:*	Yes	**No X**	NA
5.10 Will you provide a **Written Debriefing Sheet***? (if applicable)	**Yes X**	No	NA
5.11 Will you need **consent from people** who appear **in visual data** (e.g., photos or films)?*If 'yes' please provide details:* A late stage of the project will involve using pre-existing photo evidence from secured databases in order to assist with constructing an on-line tool for typologies. This will be addressed in greater detail at a future time. The photo databases used will come from partner organisations who have already established ethical standards over their use.	**Yes** **X**	No	NA
5.12 Will you **audio or video record** interviews and/or observations? *If 'yes' please provide details on how **participants' anonymity** will be maintained:* Pseudonyms will be provided with vulnerable populations in both interviews recordings and transcripts. When	**Yes X**	No	NA

necessary, software in order to alter voice/tone may be applied (i.e. vocoder)			
5.13 If the research involves**participants responding to internetsurveys, emails, chatroom discussions, blogs, interactive games, social media and networking sites etc,** how will you obtain permission from the website authors, or informed consent from participants, and ensure anonymity and protect confidentiality in an environment that generates significant amounts of background information e.g., data logs, IP addresses, cookies and caches and/or with low levels of system security? *Please provide details:* We will be working with IT specialists throughout the duration of the project who will assist with the management and operation of these problems.	**Yes X**	No	NA

Please ***submit copies of these forms *with this application*

Section 6 – Avoiding harm: risk assessment and management, safety and legal issues

6.1 Will you use an **experimental research design** (ie. implement a specific plan for assigning participants to conditions and noting consequent changes?) *If 'yes', please provide details of treatment/intervention (and specify is these are intrusive interventions e.g., hypnosis or physical exercise, or include the use of drugs, placebos or other substances e.g., vitamins, food substances etc.) and provide details of required resources for this study:*	Yes	**No X**	NA
6.2 Will the research involve **discussion of sensitive topics**? (e.g., sexual activity, drug use etc) *If 'yes' please provide details:* Issues around online abuse, particularly sexual abuse in vulnerable populations, will be central to the research. This will include issues around cyber-bullying, previous sexual exploitation, grooming, online practices, etc.	**Yes X**	No	NA
6.3 Is **pain or more than mild discomfort** likely to result from the study? *If 'yes' please provide details:*	Yes	**No X**	NA
6.4 Could the study induce **psychological stress or anxiety**or **cause harm or negative consequences** beyond the risks encountered in normal life? *If 'yes' please provide detailsand state how participants will be supported:* Some of the younger participants may be discussing elements of victimisation that could cause discomfort and distress. In addition, there is a slim possibility that victimisation is uncovered with participants as a result of the project involvement. Appropriate information will be provided in debrief to all participants for attaining additional	**Yes X**	No	NA

support. Counselling psychologists have also been worked into the grant and are available for dealing with any significant revelations and psychological difficulties.			
6.5Will the study involve prolonged and repetitive testing? *If 'yes' please provide details, justification and state how participants will be supported and length of each **data collection session**, number of sessions and location of data collection:*	Yes	**No X**	NA
6.6 Will this research be conducted **off-site** (i.e., not on MU premises)? *If 'yes', please provide details of other locations and complete a Risk Assessment Form for Fieldwork[xvi] to be submitted with this form.* This will vary greatly—both with MDX and partners and will need to be updated as the project progresses. *If 'no', a risk assessment form will need to be completed if the research involves groups of participants and there is a need to control space risks or to comply with relevant license(s).*	**Yes X**	No	NA
6.7 Will you **be alone** with individual participants or group of participants place you at risk? *If 'yes' please state how this can be avoided or managed?*	Yes	**No X**	NA
6.8 Is the research or outputs from the research **likely to cause harm** to others (e.g., to their physical well-being, mental health, dignity or personal values)to an extent greater than that encountered in ordinary life? *If 'yes' please state how this can be avoided or managed?*	Yes	**No X**	NA
6.9 Are there any **adverse risks** or **safety issues** from **potential hazards** that your methodology raises for you and/or for your participants? *If 'yes', please specify and with details of mitigating actions that will be taken*(e.g., travelling alone, working in hazardous conditions, etc.*)and how will you, and your participants/third parties be supported?*	Yes	**No X**	NA
6.10 Is this research likely to have a **damaging effect on the environment e.g., damage to habitats, plants**, or **sites** of **archaeological** or **geological** or **cultural** significance? Or a **negative impact on people living/working in** the **immediate locality** of the study? *If 'yes' please provide details and state how damage will be minimised:*	Yes	**No X**	NA
6.11 Will this research require a current **Disclosure and Barring Service** (DBS) Certificate*? **Needed when working with under-16yr olds and/or vulnerable adults for example, in education or healthcare contexts.*	**Yes X**	No	NA

Section 7 – Research Sponsorship and/or Collaboration

7.1 Does the research have a **sponsor** (i.e., any person or organisation who provides support for the research in the form of income, use of data, facilities, materials, assistance with data collection etc) that may have **ethical implications for the research**? *If 'yes' please provide details:*	Yes	**No** **X**
7.2 Does the research involve an **international collaborator** or research conducted **overseas**? *If 'yes', what ethical review procedures must this research comply with for that country, and what steps have been taken to comply with these: (e.g., Do you need local permission/approval? Are there any country specific cultural social or legal considerations that need to be taken into account? Who willbe collecting the data overseas? Have you considered intellectual property issues?)* All partner organisations will base their ethics approval process and documentation on this current form. Partners will be responsible for ensuring that their involvement throughout the project in relation to work packages and ethics are submitted and assessed by their individual institutions. As all partners are acadmeic institutions, ethic procedures will be similar to that of Middlesex. The team at Middlesex will ensire central management of partner institutions and ensure that submissions and forms meet deadlines.	**Yes** **X**	No
7.3 Does this research require **Approval from an External Research Ethics Committee**? *(e.g., Some organisations, agencies and local authorities require this*[xvii]*If 'yes' please provide details:* External ethics with various police forces (i.e. MPA in the UK) will likely be required for access to police officers. School/Educational services may also require documents to be processed in order for access to youth/students. Partner institutions will pursue parallel ethics procedures for data collection and will provide confirmations to the team at MDX when available.	**Yes** **X**	No
7.4 Will this research or part of it be conducted in a language **other than English**? *If 'yes', full translations of all non-English materials will need to be submitted.* This will be undertaken in conjunction with partner organisations (Italy and Netherlands) and they will take the lead on translations. Copies will be provided to the ethics board.	**Yes** **X**	No

Section 8– Other Issues – to be completed by ALL applicants

8.1 Does the research involve any **ethical and/or legal issues not already covered** that should be taken into consideration? *If 'yes' please give details:*	Yes	**No X**
8.2 Do you or your researchers require training on the requirements of the **Data Protection Act for researchers**?	Yes	**No X**
8.3 Does the research raise **any other risks to safety for you or others** that would be greater than in normal life? *If 'yes' please complete the MU Risk Assessment Form for submission to the REC with this form.*	Yes	**No X**
8.4 Will participants receive any **reimbursements or payments**for participating? *If 'yes' please provide details and justification:*	Yes	**No X**
8.5 Are there any **conflicts of interests to be declared** in relation to this research? *If 'yes' please complete the MU: Code of Practice for Research Appendix 2- Disclosure of Potential Conflict of Interest form for submission to the REC with this form.*	Yes	**No X**

Section 9: Declaration – to be completed by ALL applicants

As principal investigator or student researcher I confirm that:

1. I have read and agree to abide by the relevant Code(s) of Ethics appropriate to my research field and topic.
2. I have reviewed the information provided in this form and believe it accurately represents the proposed research.
3. I have read and agree to abide by the University's *Code of Practice For Research: Principles and Procedures.*
4. I agree to inform my Supervisor/Research Ethics Committee of any adverse effects or changes to the research procedures.
5. I understand that research/data may be subject to inspection for audit purposes and I agree to participate in any audit procedures required by the Research Ethics Committee (REC) if requested.
6. I understand that personal data about me contained in this form will be managed in accordance with the Data Protection Act.
7. I have completed and signed a risk assessment for this research study (if applicable).

Principal Investigator: Prof Julia Davidson **Signature**: Julia Davidson **Date**: 28th August 2014

As supervisor I confirm that:

1. I have reviewed all the information submitted with this research ethics application and believe it accurately represents the proposed research.
2. I accept responsibility for guiding the applicant so as to ensure compliance with the terms of the protocol and with any applicable Code(s) of Ethics.
3. I understand that research/data may be subject to inspection for audit purposes and I agree to participate in any audit procedures required by the Research Ethics Committee (REC) if requested.
4. I confirm that it is my responsibility to ensure that students under my supervision undertake a risk assessment to ensure that health and safety of themselves, participants and others is not jeopardised during the course of this study.
5. I understand that personal data about me contained in this form will be managed in accordance with the Data Protection Act.
6. I have seen and signed a risk assessment for this research study (if applicable).

Supervisor's Name: ..... **Signature**: ..... **Date**: .....

Please submit to your relevant Research Ethics Committee.

Please indicate which documents will be submitted

Please check and attach the following documents where applicable:			
1. Evidence of external approval – from external ethics body **(Tender acceptance in Appendix A)**	**Yes**	No	NA
2. Evidence of external approval – for access to secondary data	Yes	No	**NA**
3. Letter of permission (if required from organisation where research is to be conducted)	Yes	No	**NA**
4. Participant Information Sheet**(FOR STAKEHOLDER INTERVIEWS—Appendix B)**	**Yes**	No	NA
5. Written Informed Consent Sheet	Yes	No	**NA**
6. Written Debriefing Sheet	Yes	No	**NA**
7. Completed Risk Assessment Form	Yes	No	**NA**
8. Copy of questionnaire/interview guide/details of materials for data collection (including translations, visual images etc.)**(SCHEDULE FOR STAKEHOLDER INTERVIEWS—Appendix B)**	**Yes**	No	NA
9. Disclosure of Conflict of Interests (if applicable)	Yes	No	**NA**
10. Evidence of relevant license for research with animals/animal by-products	Yes	No	**NA**

FOR RESEARCH ETHICS COMMITTEE (REC) USE ONLY **Date:**

Reviewer's decision*(Please avoid revealing the reviewer's identity if possible)*		
1. Approved subject to the following: The only issue raised was around the suggestion that organisations that are asked to report good practice etc are being promised anonymity, but it was not clear to us if/how this can be assured if they are case studies. Is it the individuals you talk to won't be named or that the organisations won't be named? I would think if it is 'good practice' the organisation might want to be named. Can you also confirm that all the partners will go through the ethics process, that they will use the MDX ethics application as a template in seeking approval from their institutions, that any comments made about the research /any changes suggested through their ethics process will be reported to the MDX committee, and that you will hold signed copies of their ethics for your reference.	**Yes**	No
Response (1) you are correct--the individuals within the organisations will be anonymised however, from previous practice, they will be reluctant to have their industry identity revealed, therefore this will also be anonymised. We will refer to the organisations appropriately (i.e. a large, international social networking platform; we software developer, etc.). (2) again, you are correct--the partners have all been forwarded our ethics document, with appendices and will amend as needed for their own. Ethics confirmations will be kept on file and any issues arising will be fed back through our own forms. I will keep a record of all information.		

Approved by:

Dr S. Bradshaw

Chair of School of Law Ethics Committee

10/09/14

NOTES FOR COMPLETING THIS FORM

[i] ***MU Code of Practice for Research: Principles and Procedures*** *is available on the MU intranet and internet*

[ii] *See list of* ***Research Ethics Committee Contacts List*** *on the intranet and internet for submission process details*

[iii] ***Required accompanying documents*** *include the following:*

1. *Participant information sheet*
2. *Informed consent sheet*
3. *Debriefing information*
4. *Risk assessment form (required if research is to be conducted away from MU property. Institutions/locations listed for data collection must match original letters of acceptance.)*

[iv] *Please note that a student (UG, PG taught or research) cannot be the Principal Investigator for ethics purposes*

[v] *Refer to* ***Middlesex University: Definition of Research***

[vi] ***Human participants*** *are defined as including living human beings, human beings who have recently died (cadavers, human remains and body parts), embryos and foetuses, human tissue ad bodily fluids, and human data and records (such as, but not restricted to medical, genetic, financial, personal, criminal or administrative records and test results including scholastic achievements). All data collection involving human participants and/or personal data and/or sensitive personal data must receive ethics approval prior to the research commencing, with the exception of the following, which are not considered 'research': a) routine audit, b) performance reviews, c) quality assurance studies, d) testing within normal education requirements, e) literary or artistic criticism. Ref: ESRC (FRE, 2012).*

[vii] *The* ***Middlesex University Statement on Research with Animals*** *is available on the intranet and internet*

[viii] *Sources available in the public domain include published biographies, newspaper accounts, published minutes of meetings.*

[ix] *Refer to* ***Middlesex University: Definition of Research*** *section on secondary data analysis.*

[x] *The* ***Integrated Research Application System*** *(IRAS) will be applicable to research in the Confidentiality Advisory Group (CAG), National Offender Management Service (NOMS), NHS, and other health and social care / community care research review bodies in the UK. See https://www.myresearchproject.org.uk for accessing the IRAS system.*

[xi] *If* ***MU liability sponsorship*** *is required please complete all sections of this form*

[xii] *Under the* ***Computer Misuse Act*** *(1990) and the* ***Data Protection Act*** *(1998)*

[xiii] ***Human Tissue*** *(under the Human Tissue Act, 2004) refers to 'relevant material' that contains at least a single cell from a human body, e.g., organs, blood, serum, bodily waste products, cell deposits or tissue sections. (It does not include embryos outside the human body or hair and nail from the body of a living person.)*

[xiv] *For research involving* ***Human Tissue (including blood etc.)*** *please use the form and process for the Natural Sciences Department. For* ***psychological research*** *please use the forms and process for the Psychology Department.*

[xv] *The* ***Middlesex University Statement on Research with Animals*** *is available on the intranet and internet*

[xvi] *The* ***Middlesex University Risk Assessment Form*** *is available on the intranet and internet*

[xvii] ***External ethics approval*** *is required from some organisations, agencies and local authorities that have their own ethics processes and require completion of additional ethical approval forms and processing in addition to the MU process. It is your responsibility to check whether additional permissions apply to you.*